

IJCSIS Vol. 14 No. 2, February 2016
ISSN 1947-5500

International Journal of Computer Science & Information Security

© IJCSIS PUBLICATION 2016
Pennsylvania, USA

Indexed and technically co-sponsored by :



AUTHOR SERIES



IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS

International Journal of Computer Science and Information Security (IJCSIS) January-December 2016 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.

See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: see web site

Notification: see web site

Revision: see web site

Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge

Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site <https://sites.google.com/site/ijcsis/>

arXiv.org Google scholar

SCIRUS
search engine for science

ScientificCommons

Scribd

docstoc
find and share professional documents

BASE
Bielefeld Academic Search Engine

CiteSeer^x beta

dblp.uni-trier.de
Computer Science
Bibliography

DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS

EBSCO
HOST

ProQuest

For more information, please visit the journal website (<https://sites.google.com/site/ijcsis/>)

Editorial

Message from Editorial Board

It is our great pleasure to present the **February 2016 issue** (Volume 14 Number 2) of the **International Journal of Computer Science and Information Security (IJCSIS)**. High quality survey and review articles are proposed from experts in the field, promoting insight and understanding of the state of the art, and trends in computer science and technology. The contents include original research and innovative applications from all parts of the world. According to Google Scholar, up to now papers published in IJCSIS have been cited over 5668 times and the number is quickly increasing. This statistics shows that IJCSIS has established the first step to be an international and prestigious journal in the field of Computer Science and Information Security. The main objective is to disseminate new knowledge and latest research for the benefit of all, ranging from academia and professional communities to industry professionals. It especially provides a platform for high-caliber researchers, practitioners and PhD/Doctoral graduates to publish completed work and latest development in active research areas. IJCSIS is indexed in major academic/scientific databases and repositories: Google Scholar, CiteSeerX, Cornell's University Library, Ei Compendex, ISI Scopus, DBLP, DOAJ, ProQuest, Thomson Reuters, ArXiv, ResearchGate, Academia.edu and EBSCO among others.

On behalf of IJCSIS community and the sponsors, we congratulate the authors and thank the reviewers for their dedicated services to review and recommend high quality papers for publication. In particular, we would like to thank the international academia and researchers for continued support by citing papers published in IJCSIS. Without their sustained and unselfish commitments, IJCSIS would not have achieved its current premier status.

"We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication." For further questions or other suggestions please do not hesitate to contact us at ijcsiseditor@gmail.com.

A complete list of journals can be found at:
<http://sites.google.com/site/ijcsis/>

IJCSIS Vol. 14, No. 2, February 2016 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):



Open Access This Journal is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source.



Bibliographic Information

ISSN: 1947-5500

Monthly publication (Regular Special Issues)

Commenced Publication since May 2009

Editorial / Paper Submissions:

IJCSIS Managing Editor

[\(ijcsiseditor@gmail.com\)](mailto:ijcsiseditor@gmail.com)

Pennsylvania, USA

Tel: +1 412 390 5159

IJCSIS EDITORIAL BOARD

Editorial Board Members	Guest Editors / Associate Editors
Dr. Shimon K. Modi [Profile] Director of Research BSPA Labs, Purdue University, USA	Dr. Riktesh Srivastava [Profile] Associate Professor, Information Systems, Skyline University College, Sharjah, PO 1797, UAE
Professor Ying Yang , PhD. [Profile] Computer Science Department, Yale University, USA	Dr. Jianguo Ding [Profile] Norwegian University of Science and Technology (NTNU), Norway
Professor Hamid Reza Naji , PhD. [Profile] Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran	Dr. Naseer Alquraishi [Profile] University of Wasit, Iraq
Professor Yong Li , PhD. [Profile] School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China	Dr. Kai Cong [Profile] Intel Corporation, & Computer Science Department, Portland State University, USA
Professor Mokhtar Beldjehem , PhD. [Profile] Sainte-Anne University, Halifax, NS, Canada	Dr. Omar A. Alzubi [Profile] Prince Abdullah Bin Ghazi Faculty of Information Technology Al-Balqa Applied University (BAU), Jordan
Professor Yousef Farhaoui , PhD. Department of Computer Science, Moulay Ismail University, Morocco	Dr. Jorge A. Ruiz-Vanoye [Profile] Universidad Autónoma del Estado de Morelos, Mexico
Dr. Alex Pappachen James [Profile] Queensland Micro-nanotechnology center, Griffith University, Australia	Prof. Ning Xu , Wuhan University of Technology, China
Professor Sanjay Jasola [Profile] Dean, School of Information and Communication Technology, Gautam Buddha University	Dr. Bilal Alatas [Profile] Department of Software Engineering, Firat University, Turkey
Dr. Siddhivinayak Kulkarni [Profile] University of Ballarat, Ballarat, Victoria, Australia	Dr. Ioannis V. Koskosas , University of Western Macedonia, Greece
Dr. Reza Ebrahimi Atani [Profile] University of Guilan, Iran	Dr Venu Kuthadi [Profile] University of Johannesburg, Johannesburg, RSA
Dr. Umar Ruhi [Profile] University of Ottawa, Canada	Dr. Zhihan Iv [Profile] Chinese Academy of Science, China
Dr. Vahid Esmaeelzadeh [Profile] Iran University of Science and Technology	Prof. Ghulam Qasim [Profile] University of Engineering and Technology, Peshawar, Pakistan
Dr. Jiliang Zhang [Profile] Northeastern University, China	Prof. Dr. Maqbool Uddin Shaikh [Profile] Preston University, Islamabad, Pakistan
Dr. Jacek M. Czerniak [Profile] Casimir the Great University in Bydgoszcz, Poland	Dr. Musa PEKER [Profile] Faculty of Technology, Mugla Sitki Kocman University, Turkey
	Dr. Wencan Luo [Profile] University of Pittsburgh, US

TABLE OF CONTENTS

1. Paper 31011608: Implementation of RFID Technology to Improve Efficiency of Serving Customers - A Kenya Supermarket Case Study (pp. 1-5)

David Atula Luvaha, Erick Ayienga

School of Computing and Informatics, School of Computing and Informatics, University of Nairobi, Nairobi, Kenya

Abstract — Supermarkets in Kenya use the barcode technology in inventory management. If customers are many, it leads to long queues at the till thus adversely affecting efficiency of serving customers. In trying to address the queuing problem, a prototype based on RFID technology was designed with a view of improving the efficiency of serving customers. The study was about the implementation of RFID technology to improve efficiency of serving customers using a Kenya supermarket as a case study. The objectives of the study were: To design the system, to develop RFID Technology shopping cart/basket, till and the Cart Management Module (CMM) and to evaluate the system. A prototype called CMM was designed and tested. It worked as the Point of Sale (POS) System as well as automatically collected data on the shopping, queuing, transaction, packing, total transaction and total shopping durations. CMM worked hand in hand with two RFID readers namely the Check in /Checkout and till RFID readers. The data was analyzed using descriptive statistics. The results were: mean shopping duration of 3.36, mean queuing duration of 1.68, mean transaction duration of 2.73, mean packing duration of 2.63, mean total transaction time of 2.83 and mean total shopping time of 3.96 seconds. Last but not least the Old system that uses the barcode technology had a mean QD of 287 seconds. It was concluded that RFID technology improves efficiency of serving customers by drastically reducing time spent by customers in the supermarket.

Keywords-Prototype, Cart Management Module, RFID, Shopping Durations, Queuing Durations, Transaction Durations, Packing Durations, Total Transaction Time and Total Shopping Time, supermarket component

2. Paper 31011640: Face Recognition: Synthesis of Classification Methods (pp. 6-10)

Abdellatif Hajraoui, Faculty of Science and Technology, University Sultan Moulay Slimane, Beni Mellal 23000, Morocco

Mohamed Sabri, Faculty of Science and Technology, University Sultan Moulay Slimane, Beni Mellal 23000, Morocco

Mohamed Fakir, Faculty of Science and Technology, University Sultan Moulay Slimane, Beni Mellal 23000, Morocco

Abstract — Face recognition is a very active domain in computer vision and in Biometrics. It is a biometric modality that has attracted huge interest in the automatic processing of digital images and videos in many applications, including biometric identification, video-surveillance, human-computer interaction and multimedia data management. Face recognition usually involves three key processes in its treatment: face detection, feature extraction and classification. In this article, we focus on the study and synthesis of the classification methods most widely used in face recognition, namely: metric distances, neural networks and Supports Vectors Machines (SVM).

Keywords - face recognition, feature extraction, classification, metric distances, neural networks, Supports Vectors Machines (SVM).

3. Paper 31011642: A Fuzzy Logic Model for Credit Risk Rating of Egyptian Commercial Banks (pp. 11-18)

Nagy Ramadan Darwish, Department of Computer and Information Science, Institute of Statistical Studies and Research, Cairo University, Egypt

Abdelghany Salah Abdelghany, Department of Information Systems, Higher Technological Institute, Cairo, Egypt

Abstract — Credit risk rating is a method of measuring the credit worthiness in enterprises and banks by analyzing their historical data. Credit risk rating is one of the most important problems in finance. Most Egyptian commercial banks unable to determine and predict for credit risk rating and so far there is no accurate model in Egypt for determining and predicting for credit risk rating of these commercial banks. In this paper, the researchers propose a fuzzy logic based model that can be used to assist in determining and predicting for bank credit risk rating. Taking the rating scale of Moody's as an output for the proposed model. The proposed model is based on financial ratios used in Egyptian commercial banks i.e. profitability, debt-paying ability, operation ability and liquidity in order to determine their credit risk rating. This model was implemented using fuzzy logic in MATLAB and applied on CIB Egyptian commercial bank. This model could help the decision makers in the Egyptian commercial banks to determine accurately the credit risk rating of these banks.

Keywords: Machine Learning, Fuzzy Logic, Defuzzification Financial Indicators, Credit Risk Rating.

4. Paper 31011643: Performance Evaluation of Sigmoid loss for Functional and Geometric Margin Based MCE in Robust Speech Recognition (pp. 19-24)

Syed Abbas Ali, Dept. of Computer & Information Systems Engineering, N.E.D University of Engineering & Technology, Karachi, Pakistan

Adiba Jafar, Dept. of Computer Systems Engineering, Usman Institute of Technology, Karachi, Pakistan

Abeer Javed Syed, Dept. of Computer Systems Engineering, Sir Syed University of Engineering & Technology Karachi, Pakistan

Kamran Khanzada, University of Karachi Karachi, Pakistan

Abstract —This paper presents demonstrative experiments to evaluate the performance of sigmoid loss function in term of percentage error for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in the presence of three presence of three different noises (White, Pink, and Brown) with SVM classifiers using recorded and pre-conditioned speech data samples. The experimental framework consists of TI-Digit corpus and recorded digits taken from real environment with conventional and geometric SVM classifier in the presence of three different types of noises taken from NOISEX-92 noise-in-speech database. Experimental results demonstrated that average percentage error values of sigmoid loss function in GM-MCE is substantially less in comparison with percentage error values of FM-MCE for all isolated TI-Digit and recorded digit (0-9). Whereas, noise tolerance capability of GM-MCE based sigmoid loss function is considerably better than conventional FM-MCE based sigmoid loss function.

Keywords-component; Statistical Learning, Margin Based Learning, Functional Margin, Geometric Margin, Automatic Speech Recognition.

5. Paper 31011648: Comparative Study of Enhanced LIE, NPN & DES Algorithm (pp. 25-29)

*Mrs. Mukta Sharma #, Dr. R B Garg, Professor **

*#Research Scholar, TMU, *Ex-Professor, University of Delhi*

Abstract - The man has covered a long way from Stone Age to E-age (Electronic). Today, we live with technology. Technology has bridged the time and made our lives much easier. With the advent of technology, one can share their pictures, videos, money, emails etc. at a click of a button. Technology has so many advantages like one can navigate and check the routes, the nearest hotels, movie halls etc. ; can search for anything, can interact very easily with a person sitting 1000 of miles away, check the weather forecasts, transfer the money, shop online and so on. Everything comes with its pros and cons and so does the information technology. It has its own set of limitations like virus infection, hacking, spoofing, phishing, net extortion etc. One of the major fears is to transact online, there is a sense of insecurity of getting hacked and exploited. Researchers are working on ensuring the security while transacting online. One of the most significant topics of today is Cryptography. Cryptography is a technique to scramble the message into an unreadable message. Cryptography is a way of securing the message from unauthentic users. In case, an unknown person retrieves the message by hacking the system the person should not be able to read the real message.

This paper focuses on the need for cryptography, how cryptography can help saving the online transactions. A new symmetric key encryption algorithm named LIE (Let it Encrypt) has been designed using Java 1.6 (Eclipse, an IDE was used for its implementation). The paper commences with the basic introduction about security, security goals, mechanisms, cryptography, steganography etc. The paper is tactically divided into 4 sections. The first section comprises of the basic overview & structure of the algorithm. The second section depicts the implementation part, explains the code of the algorithm. Followed by its screenshots and in the end, a comparative analysis is illustrated depicting time and space for DES, NPN, and LIE algorithm.

Keywords— Cryptography, Symmetric & Asymmetric Cryptography, Plain Text, Cipher Text, DES, AES, NPN, LIE

6. Paper 31011651: Legacy Program Estimation (pp. 30-34)

Harmeet Kaur, Research Scholar, Punjab Tech. University Jalandhar, India.

Shahanawaj Ahamad, Asstt. Professor, College of Computer Science & Engineering, University of Ha'il, K.S.A.

Govinder N. Verma, Professor & Principal, Sri Sukhmani Institute of Engg. & Technology, Dera Bassi, Punjab, India.

Abstract — Software metrics support various complexity estimation techniques. This paper shows that how a set of software metrics can be used to evaluate the complexity of the legacy system. The paper presents the development of a framework and its applications. The metrics can be used in the measuring the complexity the software. To measure the decrement in complexity is one of the goals of the estimation process. As the legacy software systems are an important asset of the organization so they cannot be ignored or discarded. The collection of metrics has been used to estimate the complexity of the legacy software system to make decision on the reengineering of the legacy software. This paper demonstrates a metric framework which has been used for complexity estimation. The framework consists of various phases with applications on various open source programs written in C, C++ and COBOL.

Keywords- Program; Legacy; SDLC; CW; LOC.

7. Paper 31011652: GSM Based Bank Vault Security System (pp. 35-38)

Ripan Kumar Ray, Department of Electronics and Telecommunication Engineering, University of Development Alternative (UODA), Dhaka, Bangladesh

Muhammad Afsar Uddin, Department of Computer Science & Engineering, University of Development Alternative (UODA), Dhaka, Bangladesh

Syed Foysool Islam, Department of Electronics and Telecommunication Engineering, University of Development Alternative (UODA), Dhaka, Bangladesh

Abstract — Automated security system is a useful addition, where safety is an important issue. By this project a security system has been designed to protect the bank vault from thief or unauthorized person. This security system consists of four sensors, IP camera and GSM (Global System for Mobile communication) module. Sensors are Sound sensor, Motion sensor, Laser sensor and Gas sensor. GSM modem is used to send warning SMS to dedicated phone number. IP camera is utilized to monitor vault room remotely. When any of four sensors detect something wrong, then a warning SMS is automatically transmitted to a dedicated phone number and also a warning alarm turn on through Arduino microcontroller and GSM module. As a security system of bank vault has been designed and it has been tested several times and found most suitable security system.

Keywords — Arduino UNO microcontroller, GSM module, IP camera, Security system, Sensor, SMS.

8. Paper 31011658: Human Authentication based on Bioelectrical Signals (pp. 39-45)

Nastaran Maus Esafahani & Parinaz Saadat

Department of Computer Engineering, Amirkabir University of Technology, Iran University of Science and Technology, Tehran, Iran

Abstract — Human authentication based on electrical bio-signals, or bioelectrical signals, is a rapidly growing research area due to increasing demand for defining the identity of a person, with high confidence, in numerous applications in our vastly interconnected society. Studies show that bioelectrical signals can be not only employed for diagnostic purposes in medicine, but also used in human authentication since they have unique features among individuals. This article reviews examples of applying bioelectrical signals like Electrocardiogram (ECG), Electroencephalogram (EEG) and Electrooculogram (EOG) in human authentication and, up-to-date research efforts in this field. Utilizing bioelectrical signals provides a novel approach to user authentication that contains all the crucial attributes of previous traditional authentication. The most significant reasons for deployment of electrical bio-signals in user authentication include their measurability, uniqueness, universality and resistance to spoofing, while other conventional biometrics like face shape, hand shape, fingerprint and voice can be artificially generated.

9. Paper 31011602: Customer Relations Management using J48 Tree, Ranking Algorithm, and Chi-Square (pp. 46-53)

*Marzieh mohammadi, Faculty of Computer Engineering, Najafabad branch, Islamic Azad University, Isfahan, Iran
Hamid Rastegari, Faculty of Computer Engineering, Najafabad branch, Islamic Azad University, Isfahan, Iran*

Abstract — Customer relations management (CRM) integrates all business activities to identify and manage customers in order to increase sales in the long run and thus raise the value of companies. Efficient administration of CRM requires the recognition of appropriate patterns within the existing datasets. Analysis of such patterns will then enable managers and analysts to make the best possible decisions in critical situations. Pattern recognition is one of the fundamental goals of data mining techniques. Decision trees are popular data mining approaches commonly used as prediction models. The present study proposed a model which utilized both classification (based on J48 tree) and feature selection for the accurate prediction of marketing performance. The efficacy of the proposed model was evaluated in three datasets and the results were compared with other widely used data mining algorithms including the reduced-error pruning (REP) tree, random decision tree, support vector machine (SVM), and J48 tree. The results confirmed the higher precision, accuracy, and recall and lower error rate of the proposed model compared to the other four methods.

Keywords - Customer Relations Management (CRM); Feature Selection; Data mining; Classification; J48 Tree; Ranker Algorithm; Chi-square

10. Paper 31011604: Survey on Query Processing & Optimization Techniques in WSN (pp. 54-59)

Vandana Jindal, A. K. Verma, Seema Bawa

Department of Computer Science and Engg., Thapar University, Patiala, India.

Abstract — A WSN may be considered as a distributed database because of the presence of data in physically dispersed nodes constituting it. Data is extracted by various applications to serve the information needs. A number of techniques are being used or being introduced to extract data. Data extraction through queries is the most popular approach due to its ease of use. To combat the various limitations of limited power, bandwidth, node failure rate researchers are devising variants of querying interfaces. Main thrust is to achieve energy efficiency.

Keywords - Query processing; Query optimization; WSN

11. Paper 31011610: A Security Level Study in Cloud Computing (pp. 60-62)

Muzammil Nawaz, Computer Science, UET, Taxila, Pakistan

Rashid Amin, Computer Science, UET, Taxila, Pakistan

Fahad Ubaid, Computer Science, UET, Taxila, Pakistan

Abstract — The cloud computing network is based upon the shared resources by its service providers these services are like online storage facility, online processing and calculations in specific way and other services. These services are charged by the providers. The cloud service is no doubt a much facilitating service but there are many security issues involved with the same. Any user shares his data on cloud for processing and for other purposes and also connects with the cloud by maintaining a network with his own device. So these factors may cause security issues while using the cloud services. There is also very large verity of study done on the security issue related to cloud computing. This study is also for the same issue related to cloud network and their possible solutions, as well as related ideas for cloud providers and researchers.

Keywords: *cloud computing, security challenges, security, cloud services*

12. Paper 31011614: Optimization of SVM Parameters Based on MOPSO Algorithm (pp. 63-69)

Samira Shahinifar

Abstract — Parameters selection of support vector machine is a very important problem, which has high influence on the performance of support vector machine. This paper presents a Multi-Objective Particle Swarm Optimization Algorithm (MOPSO) approach to optimize the kernel parameters. In this paper, a MOPSO is designed with two conflicting objectives to be optimized simultaneously. These two objectives are based on the error rate and a ratio of number of support vectors to the number of instances of the dataset under evaluation. To evaluate the performance of the proposed method, experiments were executed on the datasets from LibSVM (library for SVM) and the results obtained were compared with NSGAII algorithm for parameters searching. The results obtained show that the proposed approach has less error rates and vector count across some of the datasets as compared to NSGAII algorithm.

Keywords: *Support Vector Machine; Multi-Objective Particle Swarm Optimization; Multi-Objective Genetic Algorithm; Parameter Selection.*

13. Paper 31011624: Neural Networks in the Medical Decision Making (pp. 70-75)

Manel Zribi, Faculty of Economic and Management, Sfax University Tunisia

Younes Boujelbene, Faculty of Economic and Management, Sfax University Tunisia

Abstract- This paper applies neural networks with an incremental algorithm as a tool to select the most relevant risk factors in the breast cancer disease. The results show that the neural approach with incremental algorithm is relevant in this research field. Using a sample of 248 Tunisian patients affected by this disease, we were able to identify the optimum combination of the factors that help reach a good predictive performance of the type of malignant and benign tumors.

Keywords - *ANN, incremental algorithm, risk factor classification*

14. Paper 31011633: Enhancing Intrusion Detection System by Reducing the False Positives through Application of Various Data Mining Techniques (pp. 76-87)

Vivek Kshirsagar, Dept. of Computer Science and Engineering, Government College of Engineering, Aurangabad, Maharashtra, India

Dr. Madhuri Joshi, Dept. of Computer Science and Engineering, Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra, India

Abstract — With the growth of cyber-attacks as observed over the last couple of decades safety, protection and privacy of information has become a major concern for organizations across the globe. Intrusion detection systems (IDSs) have thus gained important place and play a key role in detecting large number of attacks. There are a number of intrusion detection systems in market and most of them have the problem of having a relatively large number of false positives. Hence a need has arisen in the networking society of addressing the issue of false alarm and false positives and has resulted in an interest for researchers in IDS area. The main motivation of this research is in enhancing the performance of different data mining techniques to handle the alerts, reduce them and classify real attacks and reduce false positives. In this paper, the authors propose a novel hybrid model of RT and PART as to lower the rate of false positives. The algorithms are first trained for detecting attacks on KDD99 Dataset and then are tested on live traffic to classify whether the flow is normal or there are attacks. Random Tree (RT) and PART algorithms statistically validate the experimental results. The Hybrid framework on comparative analysis outperforms its counterparts and may lead to improved intelligent intrusion detection.

Keywords - C45, Detection rate, False Positives, intrusion detection, Random tree, Confusion matrix, PART

15. Paper 31011646: Bit Error Rate Performance Analysis of Channel Estimated Adaptive OFDM System (pp. 88-95)

Srinu Pyla, Assistant Professor, V P College of Engg. (A), Visakhapatnam, India

Dr. K Padma Raju, Professor & Director of DAP, J N T U University, Kakinada, India

Dr. N. Bala Subrahmanyam, Professor & HOD, V P College of Engg. (A), Visakhapatnam, India

Abstract - Modern communication systems are designed to support multiple applications such as data, voice, video and multimedia transmission, hence they require high data rate, spectral efficiency and inter symbol interference (ISI) free transmission. Orthogonal frequency division multiplexing (OFDM) meets the above requirements but fluctuations in Signal to Noise Ratio is quite common due to variations in envelope of OFDM signal which degrades system performance. System performance can be improved either by using Space time coding or Adaptive modulation (AM) schemes. In this work, adaptive modulation is considered due to its low complexity and optimum spectrum utilization over space time coding. In this scheme, channel state information (CSI) is fed to the transmitter to adopt the order of modulation in order to maintain constant bit error rate (BER) irrespective of the channel conditions. Here channel estimation has done using Least Square (LS), Minimum Mean Square Error (MMSE) and interpolation along with comb type pilot symbol assisted channel estimation algorithms. In this work, a new scheme has implemented to improve the BER performance by integrating channel estimation and adaptive modulation and this new scheme results superior performance over individual methods.

Keywords: Bit Error Rate (BER), Channel Estimation, Comb type pilot, Least Square (LS), Minimum Mean Square Error (MMSE), adaptive modulation and Signal to Noise Ratio (SNR).

16. Paper 31011654: JPEG Image Steganalysis Using Machine Learning (pp. 96-99)

Rahul Ranjan, Information Security and Cyber Forensics, SRM University, Kattankulathur, Chennai-603203, India

Ms Kirthiga Devi T., Department of Information Technology, SRM University, Kattankulathur, Chennai-603203, India

Abstract — The project deals with detection of steganography content. Steganography is the process of hiding the secret information within an ordinary message, pictures, audio or videos. To reveal such content is more important to avoid usage by criminals. This project applies an approach of supervised machine learning to detect the presence of steganographic content coded by programs like Steghide in the JPEG images.

Keywords—Steganography, Stego-images, Cover-images, Steganalysis.

17. Paper 31011655: Botnet: Switching c&c servers using RaspberryPI (pp. 100-104)

Tejas B Waghela, Information Security & Cyber Forensics, SRM University, Kattankulathur, Chennai – 603203, Chennai, India

Ms. Krithiga Devi T, SRM University, Kattankulathur, Chennai – 603203, Chennai, India

Abstract — Challenges for detection of botnet for forensic investigation is crucial because new models of botnet using different techniques are emerging everyday by lurking attackers in a deep web. Locating c&c servers of a botnet through usual methods might be useful in some cases when there are defects in the architecture & its inner implementation of botnet. In this paper several possibilities of making a different types of botnet are discussed, which can make detection of botmaster and c&c servers complex when usual botnet detection methods are used. This gives opportunities to the security professionals to explore different botnet architectures, its operations, locating c&c (command and control) servers & botmaster. It will encourage security professional for finding new techniques for detection of botnet & find the procedure for dealing with the same. A combination of various techniques and approaches can develop a new type of botnet which contains different perspectives that makes detection and location of botmaster and c&c servers intricate, which will also break open paths for the white hats to fight on such cyber weapons.

Keywords—c&c servers, Botnet, TOR Proxy, Raspberry PI.

18. Paper 31011662: Classification of Efficient Symmetric Key Cryptography Algorithms (pp. 105-109)

Shivlal Mewada, Department of Computer Science, MGCGV, Chitrakoot, Satna, India

Pradeep Sharma, Department of Computer Science, Govt. Holkar Sc. College, Indore, India

S. S. Gautam, Department of Computer Science, MGCGV, Chitrakoot, Satna- India

Abstract — Security threats have been a major concern as a result of emergence of technology in every aspect including internet market, computational and communication technologies. To solve this issue effective mechanism of “cryptography” is used to ensure integrity, privacy, availability, authentication, computability, identification and accuracy. Cryptology techniques like PKC and SKC are used of data recovery. In current work, we describe exploration of efficient approach of private key architecture on the basis of attributes: effectiveness, scalability, flexibility, reliability and degree of security issues essential for safe wired and wireless communication. The work explores efficient private key algorithm based on security of individual system and scalability under criteria of memory–cpu utilization together with encryption performance .The exploration results in AES as superior over other algorithm. The work opens a new direction over cloud security and internet of things.

Keywords— Private key (symmetric cryptosystem SKC); Public Key (Asymmetric cryptosystem PKC); wired communication; Wireless communication; variable key size (VKS).

19. Paper 31011669: Age Estimation Framework Based On Geometric & Appearance Feature-Based Methods (pp. 110-116)

Rania Salah El-Sayed, Department of Computer science Faculty of Science Al-Azhar University Cairo. Egypt

Abstract - Age estimation has become increasingly important, due to the fact it has a variety of potentially useful applications, such as forensic art, electronic consumer relationship management, security control and surveillance, cosmetology, entertainment and biometrics. In this paper we propose framework for age estimation. It's provides new insights into issue of feature extraction. We use the hybrid features, which are a combination of global and local features; Global features are obtained with Active Appearance Models (AAM). Local features are extracted with applying multiple Gabor filters to extract wrinkle feature each of which is designed based on the regional direction of the wrinkles, and then apply a local binary pattern (LBP), capable of extracting the detailed textures of skin. We conduct extensive experiments on standard Age estimation (FG-Net) database to verify the performance of proposed method. And we compare the result with other approach.

Keywords: Age estimation, local binary pattern (LBP), Active Appearance Models (AAM), Gabor filter, support vector machine (SVM), support vector regression (SVR).

20. Paper 31011601: A Joint Port and Statistical Analysis Based Technique to Detect Encrypted VoIP Traffic (pp. 117-131)

*Suneel Munir, Nadeem Majeed, Salaser Babu, Irfan Bari & Jackson Harry, University of Engineering & Technology, Taxila
Zahid Ali Masood, COMSATS Institute of Information Technology, Islamabad*

Abstract - VoIP is rapidly growing technology due to its cost effectiveness, dramatic functionality over the traditional telephone networks and its compatibility with public switched telephone network (PSTN). Detection of VoIP is important for telecommunication authorities, internet service providers, and governmental law enforcement agencies for blocking, prioritizing, monitoring and electronic surveillance. Modern VoIP applications use dynamic ports, proprietary protocols, encryption, obfuscation and anti-reverse engineering procedures leaving port-based techniques, signature-based techniques and pattern-based detection ineffective. For generic purpose, only statistical techniques can be used for better results but existing statistical analysis-based detection techniques have some limitations and cannot provide more efficient and accurate solutions. In this paper, we proposed a hybrid solution based on port number and statistical analysis using threshold values of flow statistical parameters to detect the VoIP media (voice) flows. The solution is generic, efficient, accurate, real time (to some extent) and can detect encrypted, plain and tunneled VoIP traffic. The proposed system is evaluated for accuracy, efficiency, and scalability. It has 97.165% detection rate (DR) and 2.68% false positive rate (FPR). It can detect VoIP calls from any VoIP application or protocol within 6 seconds. The proposed system shows better results and hence can fulfill the need of telecom operators and ISPs for detecting VoIP.

Keywords: VoIP, Encryption, Statistical analysis, Flow, Detection Rate (DR), False Positive Rate (FPR)

21. Paper 31011609: Comparative Study of Similarity Measures in Link Prediction Using Facebook Data (pp. 132-143)

*Faiza Khan, Department of Computer Science, University of Karachi
Madiha Fatima, Department of Computer Science, University of Karachi
Usman Tariq Alvi, Department of Computer Science, University of Karachi
Tahseen Jilani, Department of Computer Science, University of Karachi
Ubaida Fatima, Department of Mathematics, NED University of Science and Technology*

Abstract - Social networks are growing like a giant for the duration of several past years. This emergence has made a magneto effect on researchers of network analytics field. In this article, we are going to examine Link Prediction in Social Network. It is a problem that guesstimates the probability of existence of future links between any two particular nodes. In the following article, we will use four different similarity based proximity measures namely: Common Neighbor; Jaccard Index; Salton Index and Preferential Attachment. We will experiment these proximity measures on

Facebook data that has been collected from SNAP (Stanford Network Analysis Project) and find out AUC (Area Under the receiver operating Characteristic curve) to analyze accuracy.

Keywords - Social Networks Analysis, Link Prediction, Proximity Measures, Common Neighbors, Jaccard index.

22. Paper 31011613: Straight Line Delineation using Hough Transform on an Aerial Greenfield Imagery (pp. 144-148)

Babawuro Usman and Bashir Yusuf Bichi

Department of Computer Science, Kano University of Science and Technology, Wudil

Abstract - Hough Transform which could be used to link straight lines has been practically employed using Matlab as a computing tool, to delineate the straight edges of Aerial Greenfield imagery boundaries that demarcate some cadastral features. The demarcation is of utmost importance as it shows the extent and limit of each piece of land which is very crucial in Cadastral Science. In this paper, with the help of this popular transform, we have been able to successfully detect the boundaries and delineate the lands. With further perfection, the employment of these digital image processing algorithms could provide better alternative method over the hitherto ways being used in Plane Surveys.

Keywords: Hough transform, Digital imagery, Straight line, delineation

23. Paper 31011620: Big Data and Management of Governmental Services (pp. 149-152)

Omar Saeed Al Mushayt

Department of Administrative and Finance Sciences King Khalid University, Abha, KSA

Abstract - The term Big Data is different from traditional data in the sense of its nature, variety and velocity. Managing e-government services has become more challenging with the launching of big data. In this paper, we propose the effectiveness of deploying the techniques and tools of big data in the process of managing governmental services. We show that approach can help to get more quality and governance of governmental services.

24. Paper 31011623: Presenting a Traffic Management and Control System in Driver Assistance Form Based on Vehicular Networks (pp. 153-169)

Arefe Esalat Nejad, Young Researchers and Elite Club, Baft Branch, Islamic Azad University, Baft, Iran

Morteza Romoozi, Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran

Abstract - Vehicular Networks is considered a major step in the field of Intelligent Transportation System (ITS). In this technology, some equipment will be installed on vehicles and special places at roadsides which will enable the wireless communication between vehicles with each other and will provide the communication between the vehicles and roadside equipment. One of the ITS application is Traffic monitoring system. Such system enables accessing traffic videos by traffic monitoring centers to make traffic decision. However, providing traffic video for the vehicles can be appealing. This paper addresses a new application in vehicular networks and ITS which can provide this videos for drivers in a city. Each driver request timely traffic video of a location from a web server and the web server forward this request to a stream management server. This server based on current location of the requester vehicle, its speed and its direction calculates appropriate video chunks for each RSU along vehicle destination. This study aims to present a system which can bring a high accessibility for content and can provide it with an appropriate bandwidth and quality for vehicles. Due to the scalability and bandwidth limitations for its content and streaming, vehicular networks are used in this system.

Keywords: Vehicular Networks, ITS, Roadside unit, Traffic monitoring, stream management.

25. Paper 31011625: Facial Expression Recognition via MapReduce Assisted k-Nearest Neighbor Algorithm (pp. 170-186)

Jaafar Sadiq Qateef, Ammar Awad Kazm

Computer Science Department, College of Education, Wasit University, Iraq

Abstract - Accurate recognition and differentiation of the human facial expressions require substantial computational power, where the efficiency of algorithm plays a vital role. Recent advancement in the human computer interaction and object recognition in terms of facial expressions and gesture demanded realistic facial animation models, smart algorithms for massive data handling, as well as sophisticated graphical user interfaces. A rapid escalation in the photo upload to the online social networks web sites such as Facebook and Twitter is evident, where huge dataset handling became the key issue. Competent search and manipulations within a large dataset for image reproductions posed a new challenge, where standard tools cannot achieve the desired target. Often, images possessing intricate multidimensional attributes involve robust computational techniques for pragmatic recognition. Thus, developing a novel robust facial recognition platform emerged as an urgent necessity. We introduce a new algorithm for facial image tagging and classification in cloud environments using the Hadoop and MapReduce based k-nearest neighbor algorithms. Experiments are performed on 3120 images from 120 individuals (65 male, 55 female) from the AR Face Database. The efficiency of the proposed algorithm is evaluated in terms of recognition rates and processing time. Significant improvements in the performance are demonstrated.

Keywords: Facial expression recognition, MapReduce, Hadoop, k-nearest neighbor.

26. Paper 31011634: Construction of S-Box Based on Mobius Transformation and Increasing Its Confusion Creating Ability through Invertible Function (pp. 187-199)

M. Sarfraz (1), Iqtadar Hussain (2), Fateh Ali (1)*

(1) Department of Mathematics and Statistics, Riphah International University Islamabad, Pakistan

(2) Department of Mathematics, King Khalid University, Abha, Saudi Arabia

Abstract - Construction of widely held nonlinear transformation recognized as substitution box(S-box) which is responsible for security of modern block ciphers. Also this non-linear constituent establishes resistance against differential and linear attacks, as a result the S-box increases the ability of confusion of the cipher during the process of encryption. We proposed an algorithm based on specific category of Mobius transformation for the construction of secure S-box recognized as transformed S-box. Moreover this Mobius transformation relies on elements of which are generated through particular type of primitive irreducible polynomial. Afterwards, we apply invertible function on transformed Sbox for increasing its confusion creating aptitude and for cryptographically resilient S-box. This article also incorporated the assessment of the strength of constructed S-box through the utilization of renowned cryptographic properties such as non-linearity, criteria for bits independence, strict avalanche criterion, bits independence for SAC, bits independence for non-linearity, differential approximation and linear approximation probabilities.

Index Terms-Invertible Function, Mobius Transformation, Substitution Box.

27. Paper 31011641: SDN in Cellular Network and Implementation Challenges (pp. 200-215)

Md. Humayun Kabir, Department of Computer Science & Engineering University of Rajshahi, Rajshahi, Bangladesh

Abstract - Cellular data traffic has exploded in recent years, in large part due to the rapid proliferation of cellular devices such as smart phones, tablets and other Machine-to-Machine devices. New cellular technologies, like Long Term Evolution, have helped cellular providers to keep up with the traffic growth by increasing their radio access capacity. Although, it was a change in the right direction, the result appears to provide somewhat constrained enhancements in terms of reduction in complexity and improvement in flexibility. Software defined networking can simplify network management, while enabling new services. However, supporting many subscribers, frequent mobility, fine-grained measurement and control, and real-time adaptation introduces scalability challenges that future SDN architectures should address. In this article, various architectural aspects of today's and future SDN-based cellular network as well as its implementation challenges have been done.

Keywords- SDN, OpenFlow, LTE.

28. Paper 31011661: Realization of information exchange with Fibo-Q based Symmetric Cryptosystem (pp. 216-223)

Shaligram Prajapat, Computer Applications Department MANIT, MANIT Bhopal
Ramjeevan Singh Thakur, Computer Applications Department MANIT, Bhopal (MP), India

Abstract — Secured information exchange is demand of e-world. Numerous techniques are being evolved and experiment to share large files. Symmetric cryptosystem based algorithm works in this direction. In this paper we have discussed result of implementation of our proposed algorithm [11] based on Fibo-Q matrix. This algorithm employs generation using automatic variability concept. The corresponding numerical analysis and effective gain has also been noticed. This approach will not only enhance the security of information but also saves computation time and reduces power requirements that will find it's suitability for future hand held devices and online transaction processing.

Keywords - cipher; key; Enciphering; Decipherment; fibonacci; Q- matrix;, symmetric key algorithm, automatic variable key.

29. Paper 31011663: Dynamic Analysis Tool for Detecting SQL Injection (pp. 224-232)

Ahmed Khalid, Department of computer science, Community College, Najran University, Najran, KSA
Musab M. F. Yousif, Department of computer science, college of computer science, University of Nileen, Khartoum, Sudan

Abstract - In this paper the researchers introduce a simple algorithm by using dynamic code analysis tool for the web application to detect SQL injection vulnerability. The function of the proposed tool is depends on the extraction of the suspected GET and POST methods in the web application and checking the possibility of injecting SQL vulnerable statements. The proposed algorithm is tested using popular web sites online. Experiment is conducted to demonstrate the performance of proposed tool.

30. Paper 31011665: Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem (pp. 233-246)

Shaligram Prajapat & Ramjeevan Singh Thakur
Maulana Azad National Institute of Technology (MANIT), Bhopal, INDIA

Abstract - This paper presents enhanced model of security of symmetric key based cryptosystem [1]. The enhancement of model by variable keys and key exchange using parameters only approach is also presented. The issue of fixing up the minimum length of key for AVK is also a big challenge in AVK model. Selection of shorter key length leads to vulnerability/compromise of system, on the other side, larger then optimum key size would involve unnecessary

overheads and wastage of resources [2]. Further, ensuring high protection against malicious attack, is achieved through IDS software tools, that attempts to detect and prevent the system from malicious network users. Apart from these tools, various network security applications using pattern mining to extract the threat from cipher log. Faster and more efficient pattern matching algorithm to overcome the performance issue is demonstrated in [3], parameterized model of automatic variable key. Presented parameters only exchanged instead of key, has been analyzed using association rule discovery from hacker's perspective. This paper applies apriori method to investigate association rule among parameters used for generation of key and prediction of future key in the cryptosystem based on parameter only communication for AVK model [11]. In other words, the paper attempts to answer, how much the method is secure against association rule for future parameter prediction?

Index term: AVK, Symmetric Key, cryptosystem, IDS, Parameterized model

31. Paper 31011670: Assessment of Revenue in Roadside Units (RSU) in Traffic Management (pp. 247-252)

Arefe Esalat Nejad, Young Researchers and Elite Club, Baft Branch, Islamic Azad University, Baft, Iran

Abstract - Vehicular networks, besides supporting safety-oriented applications, are nowadays expected to provide effective communication infrastructure also for supporting leisure-oriented application including content sharing, gaming and Internet access on the move. This work focuses on Vehicle to Infrastructure (V2I) scenarios, where multiple content providers own a physical infrastructure of Road Side Units (RSUs) which they use to sell contents to moving vehicles. This paper studies a relevant problem in VANETs, known as the deployment of Roadside Units (RSUs). A RSU is an access points, used together with the vehicles, to allow information dissemination in the roads. Knowing where to place these RSUs so that a maximum number of vehicles circulating is covered is a challenge. We model the problem as a Maximum Coverage with Time Threshold Problem (MCTTP), and use a genetic algorithm to solve it.

Keywords: *Vehicular Network, RSU, Traffic Management, VANET.*

32. Paper 31011668: Impact of sink node position in the human body on the performance of WBAN (pp. 253-260)

Raju Sharma (1), Hardeep Singh Ryait (2), Anuj Kumar Gupta (3)

(1) IKG Punjab Technical University, Kapurthala, Punjab, India

(2) Department of Electronics and Communication Engineering, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India

(3) Department of Computer Science and Engineering, Chandigarh Engineering College, Mohali, Punjab, India

Abstract - Wireless body area networks consisting of various sensor nodes which are deployed on or in the human body to sense the vital sign of the human body. It is used to improve the QoS of life, healthcare applications and remote patient monitoring. Sensor nodes are placed on the human body; they sense the signal and send it to sink. Due to the movement of the body parts distance between the sensor node and sink increased or decreased which affect the performance of the network. In these networks routing protocols plays an important role together with position of sink node. Previous research shows that the best position to place the sink node in the human body is the center of the human body (waist). This paper analyzes the performance of routing protocol with arm movement by placing sink node at waist and compare these results with the results when the sink node is placed at the center of the network. Parameters used to compare the results are Stability period, Network lifetime, and Packet drop. Results show that stability and network lifetime is increased when the sink node is placed at center of network.

33. Paper 31011645: Formal Concept Analysis to Improve Robustness on Medical Image Watermarking Schemes in the Spatial Domain (pp. 261-269)

Muath AlShaikh, Lab-STICC (UMR CNRS 6285), University of Western Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS 93837, 29238 Brest Cedex, France

Laurent Nana, Lab-STICC (UMR CNRS 6285), University of Western Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS 93837, 29238 Brest Cedex, France

Lamri Laouamer, Department of Management Information Systems, CBE, Qassim University P.O. Box 6633, Buraidah, 51452, KSA

Anca Christine, Lab-STICC (UMR CNRS 6285), University of Western Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS 93837, 29238 Brest Cedex, France

Abstract - Digital medical image plays an important role in the field of Telemedicine, but patient privacy and other security issues are still coming under threats from unauthorized users. Watermarking has become essential and required for proving the identity of the owner, as well as authorizing use of images and also protecting copyrighted material from illegal access. Authorizing use and copyright protection as parameters of an image, especially of a medical image, are strongly related to robustness and complexity, imperceptibility and capacity as parameters of watermarking. Medical images have a special structure which comprises header and body blocks. The region of non interest (NROI) in the body of a medical image is the most suitable area for embedding watermark to prevent the degradation of the medical image. In our paper, we propose a novel watermarking approach in the spatial domain, based on formal concept analysis (FCA). FCA finds the optimal position for watermark embedding in NROI of the medical image. Our watermark is built from some existing information in the DICOM header (IODs). Experimental results indicate that the proposed approach would offer us high robustness with less complexity, imperceptible embedding and low payload compared with the existing watermarking approaches.

Keywords - FCA; Watermarking; Spatial Domain; Attacks; Robustness.

34. Paper 31011666: Providing Quality of Service in Cognitive Radio Sensor Networks: A Survey (pp.270-274)

Sima Bemaninejad, Department of Computer Engineering, Yazd Azad University, Yazd, Iran

Abstract — Cognitive radio (CR) technology is an excellent solution to use dynamic spectrum access (DSA) technique with the aim of resolving the spectrum underutilization problems and spectrum scarcity problems in networks. Nowadays, wireless sensor networks (WSNs) are utilized in enormous applications. The unlicensed ISM spectrum bands are used for data communication in WSNs in most applications. Due to event-triggered traffic type of WSNs, these networks commonly meet the spectrum shortage in transmission of event information. This problem is solved by providing the CR-equipped sensors for WSNs. These networks are named as cognitive radio sensor networks (CRSNs). On account of WSNs' applications, these networks usually have some properties like limited battery power of sensors, real-time and repetitive traffic, etc. Owing to dynamic spectrum availability in CRSNs, supporting the quality of service (QoS) on CRSNs is a great challenge. Consequently, providing the QoS in CRSNs is an essential result and considerable issue. This paper presents a survey of recent studies in providing the QoS of CRSNs. The schemes who provide QoS are classified based on three types of classifications: First, based on QoS metrics, second, based on the approach types which are cross-layer and single-layer, third, based on type of schemes which are distributed, centralized and cluster-based, in this paper.

35. Paper 31011653: iCloud and Its Security Issues in Relation with Find My iPhone (pp. 275-280)

Sanjay Agal & Sampreshita Maheshwari, Pacific University

Abstract — The iCloud technology is one of the recent and the most brilliant service created and hosted by the Apple Inc. Its main function is to serve as a backup system on all Apple products. The Find My iPhone application is the application, was formerly a part of the MobileMe architecture, which allows the users of the iPhone or other iDevices

to track the location of their iPhone or other iDevices when it gets either lost or stolen. The user of the application will be able to see the iPhone's (almost) approximate location on the map, display a message onto the iPhone, and/or play a sound on the iPhone (even if the iPhone is on the silent mode), change the password on the iPhone, and also remotely erase the contents of the iPhone. The Find My iPhone application was made free of charge with iOS 4.2.1 software update, but this was only for devices introduced in 2010 and thereafter. There was another iOS app released by Apple around June 2010, which allowed the users to locate their device from another iOS devices running on iOS 4 or later. With every upgrade to the application or the software there was a new feature added which made the application more efficient in tracking the lost or stolen device. There are similar phone finder services or applications under various names, which are equally good enough, also are available for other types of smartphones.

Index Terms— Find my phone, apple m artificial intelligence

Implementation of RFID Technology to Improve Efficiency of Serving Customers - A Kenya Supermarket Case Study

David Atula Luvaha, Erick Ayienga

School of Computing and Informatics, University of Nairobi, Nairobi, Kenya

Abstract—Supermarkets in Kenya use the barcode technology in inventory management. If customers are many, it leads to long queues at the till thus adversely affecting efficiency of serving customers. In trying to address the queuing problem, a prototype based on RFID technology was designed with a view of improving the efficiency of serving customers. The study was about the implementation of RFID technology to improve efficiency of serving customers using a Kenya supermarket as a case study. The objectives of the study were: To design the system, to develop RFID Technology shopping cart/basket, till and the Cart Management Module (CMM) and to evaluate the system. A prototype called CMM was designed and tested. It worked as the Point of Sale (POS) System as well as automatically collected data on the shopping, queuing, transaction, packing, total transaction and total shopping durations. CMM worked hand in hand with two RFID readers namely the Check in /Checkout and till RFID readers. The data was analyzed using descriptive statistics. The results were: mean shopping duration of 3.36, mean queuing duration of 1.68, mean transaction duration of 2.73, mean packing duration of 2.63, mean total transaction time of 2.83 and mean total shopping time of 3.96 seconds. Last but not least the Old system that uses the barcode technology had a mean QD of 287 seconds. It was concluded that RFID technology improves efficiency of serving customers by drastically reducing time spent by customers in the supermarket.

Keywords-Prototype, Cart Management Module, RFID, Shopping Durations, Queuing Durations, Transaction Durations, Packing Durations, Total Transaction Time and Total Shopping Time, supermarket component

I. INTRODUCTION

Western and European countries have used Radio Frequency Identification (RFID) technology to successfully enhance customer service and achieve increased profitability. The technology helps them ensure that goods are at the right location when customers need them and their inventories are kept up to date. However, it would be unwise for us to simply adopt such best practices and apply them in Kenya because in our environment, customers have different cultures, traditions and value systems on how they do their shopping. Therefore, it is important for us to fully study and understand how RFID technology can be used to solve typical Kenyan problems. Kwok, et al (2007) as cited by Ting et al (2011) explains that RFID technology is a non-contact and automatic identification technology that uses radio signals to identify, track, sort and

detect a variety of objects without direct contact or line of sight contact. This study seeks to find out how the powerful capabilities of the RFID technology can be harnessed and applied in inventory management in a Kenya supermarket situation to the advantage of the customers. It is for this reason that the study focuses on the Implementation of RFID Technology to improve efficiency of serving customers in supermarkets.

II. LITERATURE REVIEW

Different scholars have come up with different models in trying to solve the queuing problem in retail stores. Miwa & Takakuwa (2008) in their study called “simulation modeling and analysis for in-store merchandizing of retail stores with enhanced information technology”, proposed and constructed a simulation model of customer behavior. They used the model to examine the customer waiting times at the cash register in a retail store. In their model the customer’s movements were examined, and simulated. The simulation model was designed and developed to make use of POS data. The simulation programs were written in Arena Kelton et al, (2007). The proposed model comprised of three major logical subsystems, that is, Time Control subsystem designed to create entities or customers. Category Allocation subsystem designed to read the location of gondola display and Customer Flow subsystem designed to read a series of stored POS data and to move customers inside the retail store. Their preliminary simulation experiments indicated that when customers arrived at the store, customer waiting time became longer, unless the additional cash registers and RFID system were added. They further proposed Integrated Circuit(IC) tags and layout design as a way to reduce customer waiting time and congestion. They emphasized that IC tags allows for efficiency in transaction at the register in a retail store by eliminating time taken to read barcodes of all items.

This study borrows, modifies and enhances a lot from the study of (Miwa & Takakuwa, 2008) who viewed the Customer Flow in a retail store as a linear process where a customer goes into a store, select goods, queue at the register, pays bill and departs the store. This study views the Customer Flow as a cyclical process where the customer checks in, picks the RFID Cart/basket, selects goods, pushes the

cart/basket to the RFID till, the goods are all scanned at once, the customer pays the bill, the goods are packed and the customer checks out of the supermarket as shown in figure 1.

Miwa & Takakuwa (2008) proposed and constructed a simulation model of customer behaviour to simulate how customer waiting time was affected by additional cash registers and RFID systems. The simulation programs were coded in Arena Kelton et al. (2007). In this study a prototype called Cart Management Module (CMM) that used RFID readers was designed, tested and implemented in a supermarket to improve efficiency of serving customers. The prototype was designed using visual basic 6.0, My SQL 4.1, My SQL ODBC 3.51 driver and Crystal reports 8.5.

Miwa & Takakuwa (2008) point out that it was necessary to obtain "Purchase of Sales" data instead of "POS" data. Hence, the times marked in POS data themselves could not be used in the simulation without modifications. In this study the prototype collected the correct data for each purchased stock item and the customer who purchased it in real time as the customers did their shopping hence no need for modification of data.

Last but not least, apart from the customer waiting time which was used by Miwa & Takakuwa (2008) as performance measure, in this study the Check in Time, Shopping Duration, Basket Time, Queuing Duration, Receipt Time, Packing Duration, Transaction Duration, Total Transaction Time, Total Shopping Time and Checkout Time are all measured to give more detailed information about what happens when a customer checks in and out of the supermarket.

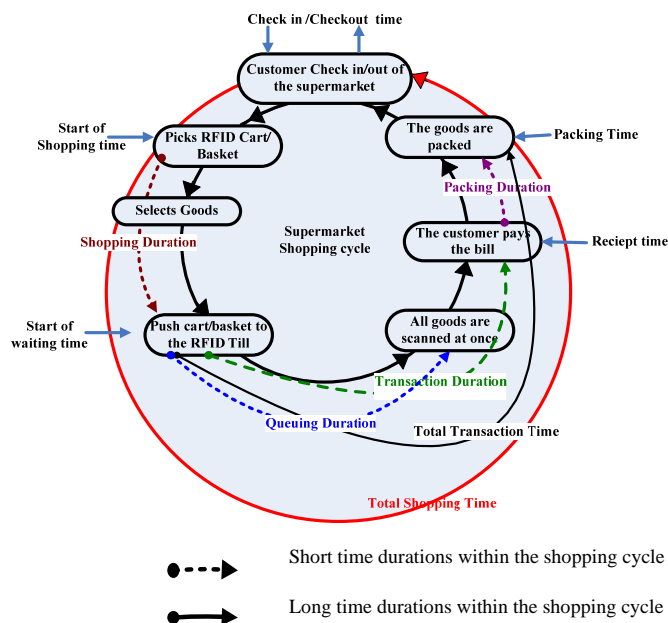


Figure 1. Shopping Cycle in Kenya Supermarket using RFID Technology, Adopted and modified from Miwa & Takakuwa, (2008)

III. METHODOLOGY AND DATA COLLECTION

The study adopted iterative research designs Wang (2012) because it is a cyclic process where a prototype is designed, tested, analyzed and refined. Based on the results of testing, changes and further refinements are then made on the most recent iteration of a design with a view of ultimately improving the quality and functionality of a design. A prototype of RFID technology Cart/basket and Cart Management Module (CMM) was designed. CMM had baskets register, stock items register, check in, RFID processing and checkout forms. The basket register form was designed to register RFID labeled shopping baskets. The stock items register form was designed to register all stock items that are RFID labeled. The check in form was designed to check in the RFID labeled shopping baskets once the customer picked it as they walked into the supermarket. The check out form was designed to check out the RFID labeled shopping baskets once the customer finished shopping and left the supermarket while the RFID processing form was designed to process the RFID labeled stock items and generate a receipt for the customer. Each form was designed, tested, analyzed, and refined. Further refinements were then made on the most recent iteration of a design to improve the quality and functionality of the design. Prototyping was used because of the benefits that prototyping offered which included the designer being able to get valuable feedback, reduced development time, reduced cost and increased user involvement in the research.

Incremental prototyping was used so that the final product is built as separate prototypes Kelly & Rector (1989). The check in and checkout forms were built, separated and designed to work with the Check in/ Checkout RFID Reader. The Check in/ Checkout Reader read the tag on the shopping basket once the customer checked in and recorded the Check in time. The check in time was assumed to be the time the shopping basket went past the check in RFID reader after the customer picked the basket and commenced shopping. This reader also recorded the checkout time which was the time the customer left the supermarket after the goods were packed. RFID processing form was designed to work with the Till RFID reader. It recorded the tag that uniquely identified the basket, all the RFID tagged stock items in the basket and the time that each and every stock item was read. All the forms including the Basket register form and stock register form were then combined together to form a complete prototype of called CMM.

Last but not least, Dynamic Systems Development Method (DSDM) life cycle was used to ensure active user involvement, quick decision making, product delivery and fitness for business purpose as the basis for which the product was assessed Chaffey (1998).

IV. RESULTS AND DISCUSSIONS

A. Analysis of the shopping Duration

The Shopping Duration (SD) is the time taken by the customer to select all preferred stock items from the shelves and place them in their shopping basket. SD was calculated by subtracting the Check in Time from the Basket Time. The Basket Time was the time the basket was placed on the RFID till by the customer so that the content of the basket is automatically read by the CMM. The SD was measured in seconds and is calculated using following formula:
Shopping Duration (SD) = Basket Time (BT) - Check In Time (CIT)

$$SD = BT - CIT$$

The mean SD and standard deviation (Std. Deviation) of SD were 3.36 and 2.442 seconds respectively. The mean SD was affected by customer preference and behavior. Majority of the customers preferred to shop up to a maximum of between 1001 – 1200 seconds. This indicates that this kind of customers like spending less time shopping. However, there was a cross section of customers who preferred to spend up to between 1401-1600, 1601-1800, 1801-2000, 3001-3200, 3201-3400 and 3401-3600 seconds.

B. Analysis of the Queuing Duration

The Queuing Duration (QD) is the time taken by the customer to stand at the till as they waits to be served. QD was ascertained by subtracting the Basket Time (BT) from Read Time (RT). The RT was the time each and every stock item was scanned by CMM through the RFID reader. Read Time was directly determined by the RFID Technology. The formula for QD is shown below:

$$\text{Queuing Duration (QD)} = \text{Read Time (RT)} - \text{Basket Time (BT)}$$

$$QD = RT - BT$$

The result is the time taken by each and every basket on the queue which is equal to time taken by the customer to queue. The QD was measured in seconds. The mean QD and the Std. Deviation were 1.68 and 1.302 seconds respectively. Figure 2 shows that majority of customers queued for ≤ 3 seconds hence positively contributing to the mean QD. The remaining customers queued for up to between 4 and 8 seconds, which was the maximum time taken by the RFID reader to read the content of the basket during the study. This was also attributed to customers having many goods on their baskets. A mean QD of 1.68 seconds and a standard deviation of 1.302 seconds indicate that RFID technology improves efficiency of serving customers in the supermarket by drastically reducing the QD to 1.68 second for each and every customer. Miwa & Takakuwa (2008) agree that IC tags ameliorate efficiency in transaction at the register.

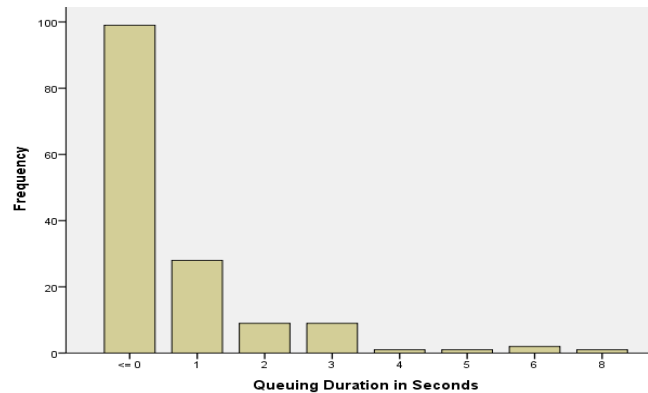


Figure 2. Customers Queuing Duration

C. Analysis of the Transaction Duration

The Transaction Duration (TD) is the time taken for the transaction to be processed using the CMM. The TD starts when the shopping basket is placed on the till and ends when the receipt is printed. TD was calculated by subtracting the Basket Time from Receipt Time (RET). The Receipt Time is the time that the receipt was generated by the supermarket attendant at the till. The formula for TD is shown below:

$$\text{Transaction Duration (TD)} = \text{Receipt Time (RET)} - \text{Basket Time (BT)}$$

$$TD = RET - BT$$

TD begins just after the QD is over. Table 1 shows that majority of the transaction took place between 6-10 and 11-15 seconds. This continues up to between 31-35 seconds due to the fact that TD is affected by human behavior. It was the supermarket attendant at the till who carried out the transactions with the aid of the CMM and Till RFID reader. It should also be noted that some customers may delay the attendant from generating the receipt by taking time to get money from their wallets after the bill has been declared. Nonetheless the mean TD and the Std. Deviation of TD was 2.73 and 1.181 seconds respectively. This contributes positively to Improving the Efficiency of Serving Customers in the supermarket. This further Indicates that RFID technology has a short TD which in turn improves efficiency of serving customers in the supermarket by drastically reducing time spent by customers on the queue while waiting for the transactions to be completed. A short TD also contributes to the customer spending less time in the shopping cycle and encourages them to come back.

Table 1. Transaction Duration for customers

TD	Frequency	Percent	Valid Percent	Cumulative Percent
<= 5	2	1.3	1.3	1.3
6 - 10	84	56.0	56.0	57.3
11 - 15	41	27.3	27.3	84.7
16 - 20	10	6.7	6.7	91.3
21 - 25	7	4.7	4.7	96.0
26 - 30	1	.7	.7	96.7
31 - 35	5	3.3	3.3	100.0
Total	150	100.0	100.0	

D. Analysis of the Packing Duration

The Packing Duration (PD) is the time taken by the packing attendant to pack the purchased stock items in paper bags or carton once the bill has been paid by the customer. This time may be affected by human factors like the fatigue, mood and morale of the packing attendant. PD may also be affected by the number, type and size of stock items purchased by the customer. It should also be noted that PD was not influenced by RFID technology used in this study because it was not used in packing the goods. PD was calculated by subtracting the Receipt Time from Check out Time. It was assumed that immediately the goods were packed, the customer walked out of the supermarket hence this time included the time taken by the customer to walk from the till to the exit of the supermarket. The formula for PD is shown below:

$$\text{Packing Duration (PD)} = \text{Check Out Time (COT)} - \text{Receipt Time (RET)}$$

$$\text{PD} = \text{COT} - \text{RET}$$

Figure 3 shows that majority of the stock items were packed between 0-50, 51-100, 101-150 and 151- 200 seconds. It is also observed that to pack some stock items, it took up to between 401 to 450 seconds. This is attributed to large quantities of assorted stock items that were being packed. However, the mean PD was 2.63 seconds while the Std. Deviation of the PD was 1.138.

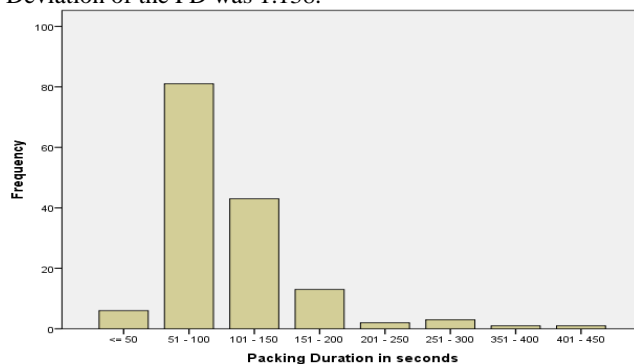


Figure 3. Customers Packing Duration

E. Analysis of the Total Transaction Time

The Total Transaction Time (TTT) is the time taken for the transaction to be processed using the RFID technology. TTT was ascertained by adding the Queuing Duration, Transaction Duration and Packing Duration. It is also calculated by subtracting the Checkout Time from the Basket Time. The formulae for TTT are shown below:

$$\text{Total Transaction Time (TTT)} = \text{Queuing Duration (QD)} + \text{Transaction Duration (TD)} + \text{Packing Duration (PD)}$$

$$\text{TTT} = \text{QD} + \text{TD} + \text{PD} \quad \text{or}$$

$$\text{Total Transaction Time (TTT)} = \text{Checkout Time (COT)} - \text{Basket Time (BT)}$$

$$\text{TTT} = \text{COT} - \text{BT}$$

TTT was determined by the speed of the RFID Technology in use, the speed of customer to paying the bill, the speeds of attendant at the till and the speed of the packing attendant. In this study, the mean TTT and the Std. Deviation of TTT were 2.82 and 1.204 seconds respectively. The mean TTT indicate that shopping using the RFID technology has a short TTT hence it improves efficiency of serving customers by drastically reducing time spent by customers on the queue while waiting for the transactions to be completed.

F. Analysis of the Total Shopping Time

The Total Shopping Time (TST) is the time taken by the customer to do shopping. This time was ascertained by subtracting the Check in Time from the Checkout Time. The formula for ascertaining the TST is shown below:

$$\text{Total Shopping Time by RFID reader (TST)} = \text{Checkout Time (COT)} - \text{Check in Time (CIT)}$$

$$\text{TST} = \text{COT} - \text{CIT}$$

TST was determined by time taken by the customer to shop, speed of the RFID Technology in use, the speed of customer in paying the bill, the speeds of attendant at the till and the speed of the packing attendant. Figure 4, shows that most of the customers took between a range of 201- 400 and 1201-1400 seconds to do their shopping. Very few customers continued to shop up to a range of 3401-3600 seconds. It is also worth noting that the availability of the RFID technology in the supermarket also contributed to the customers spending less time in the supermarket hence improving the efficiency of serving customers at the supermarket.

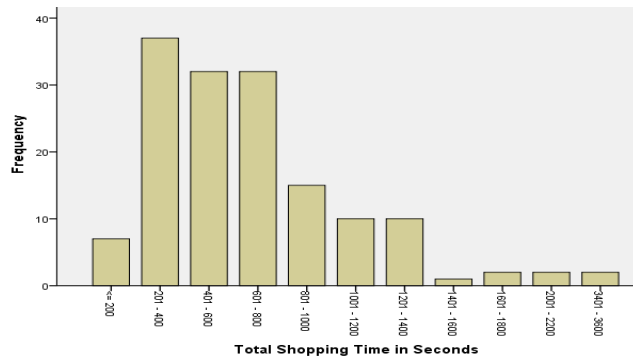


Figure 4. Total Shopping Time

G. Comparison between the Old and the New System at the Supermarket

It should be noted that the old Point of Sale (POS) system uses the barcode technology and hence it works differently as compared to the RFID POS system used in this study. Unlike the RFID Technology where tracking was possible for each and every individual stock item, in the old system individual stock items cannot be tracked hence very few parameters were measured. The system was only able to capture and store the time stamp of when the first stock item was scanned using the barcode reader and the time that the receipt was generated. The difference can be calculated and assumed to be the time that the customer queued at the till. The old system had a mean QD of 287 seconds while the new system had a QD of 1.68 seconds. This shows that the RFID system performs better than the old Barcode system in reducing queues hence improving efficiency of serving customers. Figure 5.6 shows QD using when using the Barcode Technology.

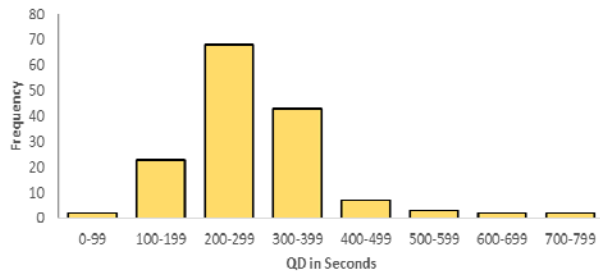


Figure 5.6: Queuing Duration using Barcode Technology

V. CONCLUSIONS

This study was about Implementation of RFID Technology to improve efficiency of serving customers- A Kenya supermarket case study. During the evaluation of the systems, the results were as follows: the mean shopping duration of 3.36 seconds, mean queuing duration of 1.68 seconds, mean transaction duration of 2.73 seconds, mean packing duration of 2.63 seconds, mean total transaction time of 2.83 seconds and mean total shopping time of 3.96 seconds. Last but not least the Old system that uses the barcode technology a mean

QD of 287 seconds. It was concluded that Implementation of RFID Technology improves efficiency of serving customers. In this study the prototype worked excellently. We recommend that a real system with all modules found in a POS be developed for commercial purposes.

ACKNOWLEDGMENT

I would like to sincerely thank all lecturers at the University of Nairobi School of Computing and Informatics (SCI) for the support they gave me while undertaking my Masters studies. It is with immense gratitude that I acknowledge the support and help of Mr. Erick Ayienga, Dr Robert Oboko, Prof. Elijah Omwenga and Prof Okelo Odongo as members of my panel. I would like to thank Mrs. Huang Wan Ming of Daily RFID for the support and guidance in the selection, purchase and shipment of RFID readers for the study. I am indebted to all sources of information used in the research and owe my deepest gratitude to all my family members and friends for their support during my studies.

REFERENCES

- [1] Calmorin, L. & Calmorin, M. (2007) *Research Methods and Thesis Writing*. In: Second Edition. [Online]. 1977 C.M Recto Avenue, Rex Book Store. p. 104. Available from: <https://books.google.co.ke/books/> [Accessed: 30 March 2015].
- [2] Chaffey, D. (1998) *Groupware, Workflow, and Intranets: Reengineering the Enterprise with Collaborative Software*. In: [Online]. 255 Wildwood Avenue Woburn, MA 01801-2041, Butterworth-Heinemann. pp. 234–235. Available from: <https://books.google.co.ke/books/> [Accessed: 30 March 2015].
- [3] Kelly, B. & Rector, A. (1989) *Research and Development in Expert Systems V*. In: [Online]. 32 East 57th street, New York, USA, The Press Syndicate of the University of Cambridge. p. 28. Available from: <https://books.google.co.ke/books/> [Accessed: 30 March 2015].
- [4] Kelton, D., Randall, S. & Deborah, S. (2007) *Simulation with Arena*. 2nd edition. [Online]. Columbus, OH 43218, Mcgraw-Hill Publ.Comp. Available from: <http://web.iitd.ac.in/~nimesh/MEL770/kelton.pdf> [Accessed: 23 March 2015].
- [5] Miwa, K. & Takakuwa, S. (2008) Simulation Modeling and analysis for in-store merchandizing of retail stores with enhanced information technology. *Proceedings of the 2008 Winter Simulation Conference*. [Online] Available from: <http://www.informs-sim.org>. [Accessed: 10 November 2013].
- [6] Sims, R. (2004) *Bivariate Data Analysis: A Practical Guide*. In: [Online]. New York, Nova Science Publishers. pp. 17–20. Available from: <https://books.google.co.ke/books?id> [Accessed: 30 March 2015].
- [7] Ting, S., Kwok, S., Tsang, A. & Ho, G. (2011) The Study on Using Passive RFID Tags for Indoor Positioning. *International Journal of Engineering Business Management*. [Online] 3. Available from: www.intechopen.com [Accessed: 22 January 2014].
- [8] Wang, J. (2012) *Advancing the Service Sector with Evolving Technologies: Techniques and Principles*. In: [Online]. 701 E. Chocolate Avenue Hershey PA 17033, Business Science Reference (an imprint of IGI Global). Available from: <https://books.google.co.ke/books?id> [Accessed: 30 March 2015].

Face recognition: synthesis of classification methods

Abdellatif Hajraoui

Faculty of Science and Technology,
University Sultan Moulay Slimane,
Beni Mellal 23000, Morocco

Mohamed Sabri

Faculty of Science and Technology,
University Sultan Moulay Slimane,
Beni Mellal 23000, Morocco

Mohamed Fakir

Faculty of Science and Technology,
University Sultan Moulay Slimane,
Beni Mellal 23000, Morocco

Abstract—Face recognition is a very active domain in computer vision and in Biometrics. It is a biometric modality that has attracted huge interest in the automatic processing of digital images and videos in many applications, including biometric identification, video-surveillance, human-computer interaction and multimedia data management. Face recognition usually involves three key processes in its treatment: face detection, feature extraction and classification. In this article, we focus on the study and synthesis of the classification methods most widely used in face recognition, namely: metric distances, neural networks and Supports Vectors Machines (SVM).

Keywords- face recognition, feature extraction, classification, metric distances, neural networks, Supports Vectors Machines (SVM).

I. INTRODUCTION

Technological progress, particularly in new information processing techniques and the imminent revolution in microprocessor systems have enabled the development of artificial solutions for recognition of human faces.

During the installation of an automated system for face recognition, the context of its field of application sets its operating mode: authentication (one to one) or identification (one to many). In the first mode, the system must verify the identity of a person by declaring him as a legitimate user or impostor. Whilst for the second, the system must affect an identity to a person from those registered or declare him as unknown. In both modes, the system must have a reference database (Gallery) that contains all the feature vectors (signatures) of faces of persons assumed known by the system. These signatures are learned during a phase called enrollment. The latter is achieved off-line by executing the key steps described hereafter and illustrated by figure 1. Furthermore, to identify or authenticate a person from his face image (query face image) in the recognition phase, the same steps have to be treated, but this time around on-line. These steps provide the following functions:

Face detection: this step used to detect the presence or absence of faces in the captured image or video. If the latter contains faces, it locates their positions and it provides in output the isolated face images of the rest of the scene. Several techniques have been proposed to solve this problem of face detection, such as: [1] [2] [3] [4].

Extraction of the feature vector: this is a crucial step in a face recognition system. This step also called indexing or modeling, allows the extraction of the face image detected the pertinent informations that characterizes it: feature vector or signature. This vector must be different from one person to another and invariant for different facial appearances of the same person. In the literature, there is a multitude of algorithms for feature extraction [5] [6] [7] [8] [9] [10].

Classification: this step permits the classification of the feature vector of the person to recognize. His treatment requires the introduction of a comparison algorithm or classification which provides at its output a score of similarity or distance between this characteristic vector and the reference feature vectors of the database (gallery). This score is compared subsequently to a decision threshold fixed in advance for provide a final decision on identity.

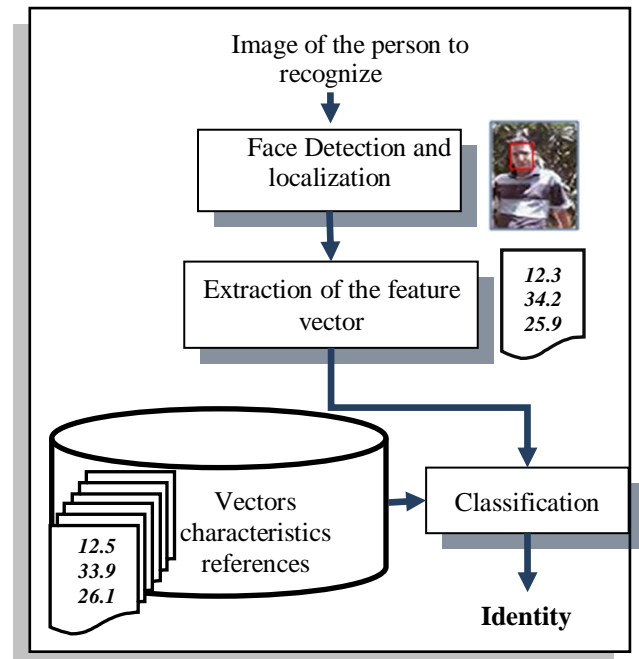


Figure 1. Basic architecture of an artificial system of face recognition

In this article, it focused in the synthesis of the most widely used methods in the classification process of a face recognition system, namely: Metric distances, neural networks and Supports Vectors Machines (SVM).

II. THE AUTOMATIC CLASSIFICATION IN FACE RECOGNITION

The automatic data classification is a branch of the data analysis and data mining which has resulted in numerous and diverse publications. It is used to group data into classes so that the data of the same class are as similar as possible and the classes are the most distinct possible.

The approaches proposed in the literature to solve the classification problem in a face recognition system come under that branch. These approaches can be classified into two categories. In the first category, there are comparison approaches that are based on the calculation of the distances between the feature vectors stored in the database (extracted off-line) and that of the person to be recognized (extracted line). In this case, the boundaries of discrimination between classes of these vectors are determined a posteriori in the recognition phase. These approaches generally exploit metric distances. While the for second category, there are methods occurs first time in the enrollment phase to determine a priori the boundaries of discrimination between classes of the database. This operation is performed by supervised learning of a classifier. And in second time, in the recognition phase to target the query face membership class using a classification technique. Among these methods: Neural Networks and Supports Vectors Machines.

Given the diversity of these approaches, the comparative analysis of their performance (speed and recognition rate) is important before taking the decision on the approach to implement because the choice depends on the functions sought by the intended application and the following constraints:

- The type of algorithm used in the feature extracting step.
- The volume of the database (gallery).
- The size of the feature vectors (signatures).

III. METRIC DISTANCES

When one wishes to compare two feature vectors $S1$ et $S2$: $S1 = (S1_1, S1_2, ..., S1_n)$ et $S2 = (S2_1, S2_2, ..., S2_n)$ resulting from the feature extraction step, one can perform a measurement of the degree of divergence between these two vectors using a metric distance. The most metric distances used in face recognition are: the Euclidean distance, the Manhattan distance, the Mahalanobis distance and the cosine distance.

A. Euclidean Distance :

$$D_2(S1, S2) = \sqrt{\sum_{k=1}^n (S1_k - S2_k)^2} \quad (1)$$

B. Manhattan Distance:

$$D_1(S1, S2) = \sum_{k=1}^n |S1_k - S2_k| \quad (2)$$

C. Mahalanobis Distance :

The Mahalanobis distance can be defined as the dissimilarity measure between two vectors $S1$ and $S2$ of the same assembly with a covariance matrix C :

$$D_{Mah}(S1, S2) = \sqrt{(S1 - S2).C^{-1}.(S1 - S2)^T} \quad (3)$$

D. Cosinus Distance

The cosine distance is used to calculate the similarity between two feature vectors by determining the cosine of the angle θ between them:

$$D_{cos}(S1, S2) = \cos(\theta) = \frac{S1.S2}{\|S1\|.\|S2\|} \quad (4)$$

Once the type of distance metric is chosen, its exploitation in the classification stage can be formalized as follows:

Either S_i the feature vector of the person to be identified. His identification consists in assigning it an identity Id_i among the M identities Id_k of the individuals previously enrolled in the system, of the individuals previously enrolled in the system, or Id_0 in the case of unknown identity. The identification function f may thus be defined:

(5)

Où S_k est le vecteur caractéristiques correspondant à l'identité Id_k , D est la distance choisie et $Seuil$ est la valeur au-dessous de laquelle la personne est identifiée comme client.

Where is the vector corresponding to the characteristics Id_k identity is selected distance and the Threshold is the value below which the person is identified as a client.

IV. NEURAL NETWORKS

A neural network is more or less complex combination of basic objects called formal neurons (figure 2). These have an activation function that allows influence other network neurons. The connections between the neurons, which is called synaptic connections, spread the activity of neurons with a characteristic weighting connection.

With their machine learning capability from data modeling the problem to solve, neural networks have been used in all the modules intervenir in the processing chain of automatic face recognition system [11] [12] [13] [14] [15].

The particular architecture of neural networks called Multi-Layer Perceptron (MLP) (the case of figure 2) is often exploited as a means of classifying feature vectors extracted from the faces. To achieve this objective, the following two procedures can be executed:

During the enrollment phase, a supervised learning of the Multi-Layer Perceptron must be carried out from the set of extracted feature vectors of the faces of the database. This type

of learning is generally performed using the back-propagation gradient algorithm.

During the recognition phase, the feature vector of the face of the person to recognize is presented to the input perceptron. The output of the latter which takes the maximum value (closer to 1) shows which class (human identity) belongs to that face.

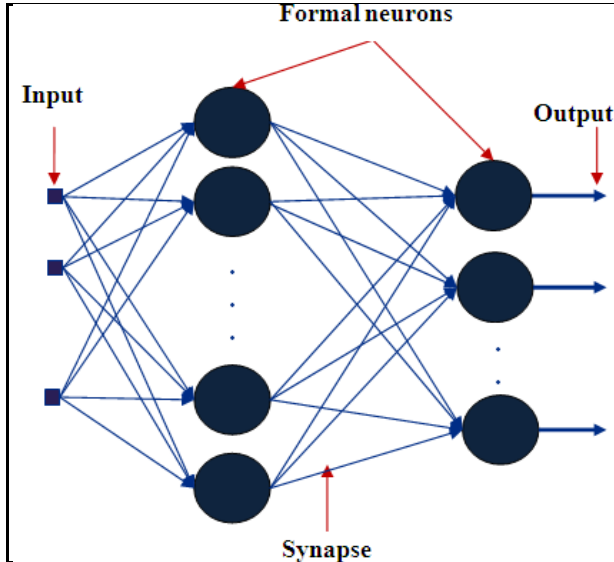


Figure 2. Example of architecture of a neural network

V. SUPPORT VECTORS MACHINES (SVM)

SVM currently attracting much attention in the community of machine learning, which proves their gain in popularity and use in many applications such as pattern recognition (handwritten scriptures, faces, ...), text categorization (classification of emails, web pages classification, ...), medical diagnosis (risk assessment of cancer, cardiac arrhythmia detection, ...),

The main objective of SVM is to find a decision boundary that separates the data points of two different classes. This boundary is called a separator, must be a hyperplane. In general, there may be multiple hyperplanes possible separators between the two classes. However, it made a particular choice among all possible separators, it seeks Optimal Separating hyperplane (figure 3). To determine the latter, closest uses only data points (the points of the boundary between the two classes of data) from the total set of learning, these points are called support vectors (support vectors). The distance between these points is called margin. It is this distance that we must maximize (maximum margin).

For details on obtaining certain mathematical formulas necessary for the implementation of the SVM or an understanding of SVM, the reader may refer to the memory of the thesis [16], the pages: 31-37 and 53-56.

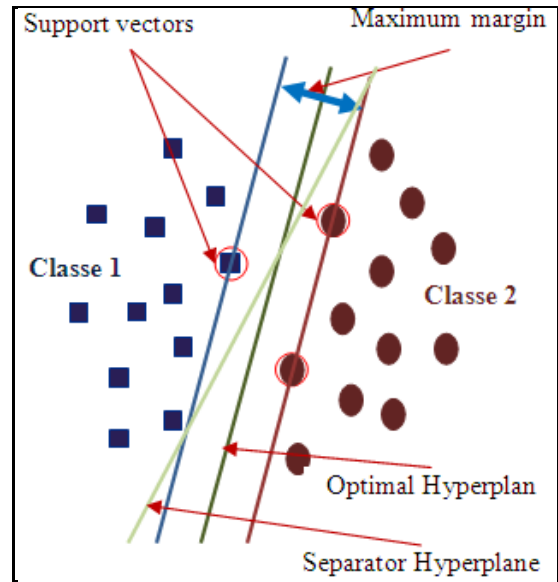


Figure. 3. Illustration des notions de base de SVM

SVM is a classification method that has proven effective in solving some problems related to the field of face recognition, such as:

- The detection of faces in an image, specifically for the face and non-face classification of objects located in an image [17][18]
- The classification of feature vectors (signatures) faces [9] [19][20].

VI. SYNTHÈSE EXPÉRIMENTALE

In the context of the performance evaluation of classification methods discussed in this article, experimental synthesis is carried out. But to confirm this assessment, on the one hand, the tests are experienced on the standard AT&T database [21] (Figure 4), and secondly we have made comparisons of these classification methods using different feature extraction algorithms: PCA [5], PCA-double LDA [9] and Gabor-PCA-double LDA [10].

Here below, the parameters of the different tools of experimental synthesis:

Reference faces (Gallery): 200 face images of the AT&T database, the first 5 images for each person (altogether 5x40).

Test faces: 200 face images of the AT & T base, the last 5 images for each person (altogether 5x40)

Multi-layer Perceptron with the architecture and the following parameters:

- One input layer where the number of input cells is equal to the size of feature vectors which depends on the extraction method evaluated.
- A single hidden layer composed of a number of neurons which is also adapted to the size of the feature vectors.

- A release layer composed of a number of neurons that is equal to the size of the gallery.
- The Sigmoid function as neuronal activation function.
- A stopping criterion of the learning algorithm which corresponds to a square error lower than a threshold of 0.0001 or a maximum number of iterations of 100,000 iterations.

SVM using:

- K. (K-1) / 2 classifiers SVM binary and non-linear (K is the number of classes (people) of the reference database (Gallery)).
- The adopted core function is to Polynomial kind.

The performances evaluated:

- The recognition rate with different classification methods (Table 1).

- The average time of identification with different classification methods (Table 2). This time is raised between the read time of the face image to be identified and the moment of decision making.
- The multi-class classification method is one against one.



Figure 4. Extract from the AT & T database

TABLE 1. RECOGNITION RATE (%)

Feature Extraction Algorithm	Classification Method					
	<i>Manhattan Distance</i>	<i>Euclidean Distance</i>	<i>Mahalanobis Distance</i>	<i>Cosinus Distance</i>	<i>MLP</i>	<i>SVM</i>
<i>PCA</i>	70.50	71.00	77.50	77.00	79.00	80.50
<i>PCA-double LDA</i>	83.00	83.00	89.50	88.00	91.50	93.50
<i>Gabor-PCA-double LDA</i>	98.00	98.00	98.50	98.00	99.00	99.00

TABLE 2. AVERAGE TIME OF IDENTIFICATION (S)

Feature Extraction Algorithm	Classification Method					
	<i>Manhattan Distance</i>	<i>Euclidean Distance</i>	<i>Mahalanobis Distance</i>	<i>Cosinus Distance</i>	<i>MLP</i>	<i>SVM</i>
<i>PCA</i>	0.0781	0.0782	0.0801	0.0782	0.0810	0.0924
<i>PCA-double LDA</i>	0.0892	0.0890	0.0907	0.0893	0.0911	0.1091
<i>Gabor-PCA-double LDA</i>	0.4974	0.4972	0.5003	0.4975	0.5015	0.5186

The results presented in Table 1 indicate that the two modern classification techniques (SVM and MLP) are better in terms of the recognition rate than traditional methods (metric distances). Also the Mahalanobis distance sees himself superior compared to other distances. It is for this reason that the majority of recent work favor the Mahalanobis distance relative to other distances.

Concerning the classification time, one notes that the metric distances guarantee the shortest time. Contrary to SVM, this time is the longest. While the Mahalanobis distance and MLP come to rank medium. Such a finding cannot be generalized. Indeed, when the classification will be performed on a database (Gallery) very large this classification of time significantly increase in cases of metric distances and SVM because these two types of methods, the number of comparisons increases

with the number of classes. However, for the MLP, this time is almost unchanged since the MLP only use in the identification phase of the matrix product calculation of the feature vector and matrix representing the weights of synapses. Accordingly, it is the MLP who will take the first rank.

VII. CONCLUSION AND PERSPECTIVES

The results obtained in this experimental synthesis claim that SVM classification guarantee the best efficiency (large classification rates) compared to metric distances and MLP neural networks. However, it is they who guarantee the best speed (a very short calculation time in the recognition phase). However, the two classification methods: MLP and SVM, have a major drawback which occurs when adding a new person in the reference database (Gallery). In such a situation, one must repeat the entire learning process, unlike techniques that use a metric distance, classify and allocate new faces without going through a learning step. This comparison gives us a starting point to make optimal choices will depend on the application.

The perspective point of view, we suggest an extension of this summary to other classification methods such as: decision trees.

REFERENCES

- [1] P. Viola and M. Jones. Robust real-time face detection. *International Journal of Computer Vision*, Vol. 57, N° 2, p.: 137–154, 2004.
- [2] H. Pan, Y. Zhu and L. Xia, Efficient and accurate face detection using heterogeneous feature descriptors and feature selection, *Computer Vision and Image Understanding*, Vol. 117, p.: 12–28, 2013.
- [3] M. H. Rahman and J. Afrin. Human Face Detection in Color Images with Complex Background using Triangular Approach. *Global Journal of Computer Science and Technology Graphics & Vision*, Vol. 13, Issue 4, pages: 45-50, 2013.
- [4] A. Hajraoui and M. SABRI. Face Detection Algorithm based on Skin Detection, Watershed Method and Gabor Filters. *International Journal of Computer Applications*. Vol. 94, N° 6, pages: 33-39, Mai 2014.
- [5] M. Turk and A. Pentland. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, Vol. 3, No. 1, p.: 71-86, 1991.
- [6] L. Wiskott, J. M. Fellous, N. Kuiger and C. von der Malsburg. Face recognition by elastic bunch graph matching. *IEEE Transactions PAMI*, Vol. 19, N° 7, p.: 775-779, Juin 1997.
- [7] N. S. Vu and A. Caplier. Face Recognition with Patterns of Oriented Edge Magnitudes. *Computer Vision (ECCV 2010)*, tome 6311 of *Lecture Notes in Computer Science*, p.: 313–326. Springer Berlin / Heidelberg, 2010.
- [8] D. Monzo, A. Albiol et J.M. Mossi. Color HOG-EBGM for face recognition. 18th IEEE International Conference on Image Processing (ICIP 2011), pages: 785 – 788, Bruxel, 11-14 Septembre 2011.
- [9] A. Hajraoui, M. SABRI, M. FAKIR and O. BENCHAREF. A new approach for Face Recognition Based on PCA & Double LDA Treatment combined with SVM. *IOSR Journal of Engineering*. Vol. 2, N° 4, pages: 685-691, Avril 2012.
- [10] A. Hajraoui, M. SABRI and M. FAKIR. Complete architecture of a robust system of face recognition. *International Journal of Computer Applications*. Vol. 122, N° 1, pages: 26-31, Juin 2015.
- [11] N. Shilbayeh and G. Al-Qudah. Face Detection System Based On MLP Neural Network. *Recent Advances in Neural Networks, Fuzzy Systems & Evolutionary Computing*, p.: 238-243, 2008.
- [12] M. Abadi. Face Detection with the Help of Gabor Wavelets Characteristics and Neural Network Classifier. *American Journal of Scientific Research*, Issue. 36, p.: 67-76, 2011.
- [13] M. Rizon, M. F. Hashim, P. Saad et S. Yaacob. Face Recognition using Eigenfaces and Neural Networks. *American Journal of Applied Sciences*, Vol. 3, N° 6, pages: 1872-1875, 2006.
- [14] M. S. S. Ranawade. Face Recognition and Verification Using Artificial Neural Network. *International Journal of Computer Applications*, Vol. 1, N° 14, pages: 23-30, 2010.
- [15] M. Agarwal. Face Recognition Using EigenFaces and Artificial Neural Network. *International Journal of Computer Theory and Engineering*, Vol. 2, No. 4, pages: 624- 629, Aout 2010.
- [16] M. Feuilloy. Study of machine learning algorithms for the prediction of syncope in humans. PhD thesis, University of Angers, 2009.
- [17] H-J. Lin, S-H. Yen, J-P. Yeh and M-J. Lin. Face Detection Based on Skin Color Segmentation and SVM Classification. Dans *Second International Conference on Secure System Integration and Reliability Improvement (SSIRI '08)*, p.: 230 – 231, 14-17 Juillet 2008, Yokohama.
- [18] S. Ravi and S. Wilson. Face detection with facial features and gender classification based on support vector machine. *International Journal of Imaging Science and Engineering*, 2010, Special Issue.
- [19] S. Meshgini, A. Aghagolzadeh and H. Seyedarabi. Face Recognition Using Gabor Filter Bank, Kernel Principale Component Analysis and Support Vector Machine. *International Journal of Computer Theory and Engineering*, Vol. 4, N° 5, Octobre 2012.
- [20] F. Bellakhddhar, K. Loukil and M. Abid. Face recognition approach using Gabor Wavelets, PCA and SVM. *International Journal of Computer Science Issues*, Vol. 10, Issue 2, N° 3, p.: 201-207, Mars 2013.
- [21] www.cl.cam.ac.uk/Research/DTG/attarchive/pub/data/att_faces.zip

A Fuzzy Logic Model for Credit Risk Rating of Egyptian Commercial Banks

Nagy Ramadan Darwish

Department of Computer and Information Science
Institute of Statistical Studies and Research
Cairo University, Egypt

Abdelghany Salah Abdelghany

Department of Information Systems
Higher Technological Institute
Cairo, Egypt

Abstract—Credit risk rating is a method of measuring the credit worthiness in enterprises and banks by analyzing their historical data. Credit risk rating is one of the most important problems in finance. Most Egyptian commercial banks unable to determine and predict for credit risk rating and so far there is no accurate model in Egypt for determining and predicting for credit risk rating of these commercial banks. In this paper, the researchers propose a fuzzy logic based model that can be used to assist in determining and predicting for bank credit risk rating. Taking the rating scale of Moody's as an output for the proposed model. The proposed model is based on financial ratios used in Egyptian commercial banks i.e. profitability, debt-paying ability, operation ability and liquidity in order to determine their credit risk rating. This model was implemented using fuzzy logic in MATLAB and applied on CIB Egyptian commercial bank. This model could help the decision makers in the Egyptian commercial banks to determine accurately the credit risk rating of these banks.

Keywords: Machine Learning, Fuzzy Logic, Defuzzification Financial Indicators, Credit Risk Rating.

I. INTRODUCTION

Credit risk rating is one of the most important problems in finance. A credit risk rating is an evaluation of the credit worthiness of a debtor. Credit ratings are issued by credit rating agencies (CRA). Companies like Standard & Poor's, Moody's and Fitch are considered the most important ones. They assign ratings for several issuers (e.g. firms, nations, local governments and banks) of specific types of debt. In this paper the focus is on the commercial banks [1, 2].

Commercial Banks (CBs) are profit-making organizations acting as intermediaries between borrowers and lenders. CBs play a critical role to emergent economies like Egypt. Bank lending is very critical for financing agricultural, industrial and commercial activities of the country. Well-functioning CBs accelerate economic growth [3].

Credit rating agencies often classify credit rating of certain Egyptian banks such as National Bank of Egypt (NBE), Banque Misr (BM), and Commercial International

Bank (CIB) and do not give a classification of all commercial banks in Egypt. Additionally, there is no accurate model in Egypt for determining and predicting for credit risk rating of these commercial banks.

Furthermore the application of machine learning techniques has been very limited in the context of economics and studies of finance. This paper highlights the importance of incorporating machine learning techniques in the assessment of credit risk rating of commercial banks.

In this paper, the researchers propose a fuzzy logic based model that can be used to assist in determining and predicting for bank credit risk rating. Taking the rating scale of Moody's as an output for the proposed model. This paper focuses on commercial banks in Egypt that have suffered from few models for credit risk rating in recent years which led to lose finance in these banks. This model could help the decision makers to the right decisions to determine the credit risk rating of these banks.

The paper is organized as follows: Section 2 shows a background overview of credit risk rating and fuzzy logic approach. Section 3 summarizes the most important studies in this research field. Section 4 presents the proposed model for credit risk rating. Section 5 introduces an algorithm of the proposed model. Section 6 presents the implementation of the proposed model. The last section concludes the paper with final remarks.

II. BACKBOARD OVERVIEW

This section provides an overview about the main concept related to the research topic. It consists of two parts. In the first part, a set of financial ratios which are used in the assessment of bank credit risk rating is presented. In the second part, the basic concept of fuzzy logic is discussed.

A. Financial Indicators for Credit Risk Rating

Credit risk rating consists of two parts, namely quantitative and qualitative indicators. Our proposed model for credit risk rating focuses on quantitative factors. The summary of financial indicators that were incorporated in the

proposed model is shown in Table 1 [4, 5]. These indicators are classified into four categories as follows:

- **Profitability:** the ability of banks to earn profit under normal operation situation reflects the degree of risk.
- **Debt-paying ability:** the ability of banks to repay the due short-term and long-term debts, which is helpful to forecast the banks potential earnings and reduces the risk of banks.
- **Operation ability:** the ability of banks using various assets to gain profits.
- **Liquidity:** the bank's ability to pay off its short-terms debts obligations.

The proposed model for credit risk rating is based on the system of rating that was originated by John Moody in 1909. The purpose of Moody's ratings is to provide investors with a simple system of gradation. Gradations of creditworthiness are indicated by nine group rating symbols as shown in Table 2. Additionally, Moody's rating system appends numerical modifiers 1, 2, and 3 to each generic rating classification from Aaa through Caa [6].

TABLE 1. THE SUMMARY OF FINANCIAL INDICATORS FOR CREDIT RISK RATING

Ratio Name	Indicator Name	
Profitability	Rate of return on capital	ROC
	Net profit margin on sales	NPM
Debt-paying ability	Current ratio	CTR
	Quick ratio	QKR
	Currency ratio	CYR
	Debt asset ratio	DTR
Operation ability	Total assets turnover	TAT
Liquidity	Securities to Assets	SA
	Deposits to Assets	DA
	Loans to Deposits	LD

TABLE 2 THE RATING CLASSES FROM MOODY'S RATING AGENCY

Symbol	Definition
.Aaa	Obligations rated Aaa are judged to be of the highest quality, subject to the lowest level of credit risk
Aa	Obligations rated Aa are judged to be of high quality and are subject to very low credit risk.
A	Obligations rated A are judged to be upper-medium grade and are subject to low credit risk.
Baa	Obligations rated Baa are judged to be medium-grade and subject to moderate credit risk and as such may possess certain speculative characteristics.
Ba	Obligations rated Ba are judged to be speculative and are subject to substantial credit risk
B	Obligations rated B are considered speculative and are subject to high credit risk.
Caa	Obligations rated Caa are judged to be speculative of poor standing and are subject to very high credit risk.
Ca	Obligations rated Ca are highly speculative and are likely in, or very near, default, with some prospect of recovery of principal and interest.
C	Obligations rated C are the lowest rated and are typically in default, with little prospect for recovery of principal or interest.

B. Fuzzy Logic

Fuzzy logic was introduced by Lotfi Zadeh in 1965. The term fuzzy logic in a broader sense can be defined as a set of

mathematical principles for knowledge representation based on degrees of membership rather than on crisp membership of classical binary logic. As such, it is a multi-valued logic [7]. Following some fuzzy basic concepts:

1) *Fuzzy Sets:* A fuzzy set is a class of objects with a continuum of grads of membership [8]. Let X be a space of points (objects) and its elements be denoted as x . A fuzzy set A of X is defined by function $f_A(x)$ called the membership function of set A :

$$f_A(x): X \rightarrow [0,1] \quad (1)$$

2) *Membership function:* A membership function $f_A(x)$ associates with each point in X a real number in the interval $[0, 1]$, with the value of $f_A(x)$ at x representing the "grade of membership" of x in A .

3) *Basic operations of fuzzy sets:* There are four basic fuzzy set operations:

- *Complement:* The complement of a fuzzy set A is denoted by A' and can be found as follows:

$$f_{A'} = 1 - f_A \quad (2)$$

- *Containment:* A is contained in B if and only if $f_A \leq f_B$. In symbols:

$$A \subset B \Leftrightarrow f_A \leq f_B \quad (3)$$

- *Union:* The union of two fuzzy sets A and B with respective membership functions $f_A(x)$ and $f_B(x)$ is a fuzzy set C , written as $C = A \cup B$, whose membership function is related to those of A and B by:

$$f_C(x) = \text{Max}[f_A(x), f_B(x)] \quad x \in X \quad (4)$$

- *Intersection:* The intersection of two fuzzy sets A and B with respective membership functions $f_A(x)$ and $f_B(x)$ is a fuzzy set C , written as $C = A \cap B$, whose membership function is related to those of A and B by:

$$f_C(x) = \text{Min}[f_A(x), f_B(x)] \quad x \in X \quad (5)$$

4) *Fuzzy rules:* A fuzzy rule is a conditional statement of the form IF A THEN B , where A and B are terms with a fuzzy meaning [9].

III. RELATED WORK

In general, several approaches have been proposed in order to establish a model that is capable of determining and predicting for credit risk rating. For example, L. Yijun, C. Qiuru, L. Ye and Q. Jin [10] proposed a neural network model to make an effective analysis for corporation credit rating. H. A. Abdou [11] conducted a study to investigate the ability of genetic programming (GP) in the analysis of credit scoring models in Egyptian public sector banks. W. Hongxia, L. Xueqin and L. Yanhui [12] proposed a model based on

fuzzy clustering and decision tree for assessing enterprise credit rating.

C. Tsai and M. Chen [13] investigated credit rating by hybrid machine learning techniques to help to decide whether to grant credit to consumers before issuing loans. Y. Wei, S. Xu and F. Meng [14] proposed a company's credit rating model based on logistic regression and non-financial factors. P. Hájek [15] conducted a study to classify US municipalities (located in the State of Connecticut) into rating classes by neural networks. V. H. Duc and N. D. Thien [16] proposed a new model to determine credit ratings for Vietnamese companies by using fuzzy logic.

F. M. Rafiei, S. M. Manzari and M. Khashei [17] used Multilayer Perceptrons (MLPs) and multiple statistics methods to carry out multi-class credit rating of listed corporations in Tehran Stock Exchange (TSE). M. R. Gholamian, S. Jahanpour and S. M. Sadatrasoul [18] presented a new method to analyze customer credit worthiness. R. H. Abiyev [19] introduced credit rating model using type-2 fuzzy neural networks (FNN). N. Shovgun [20] suggested a new method based on fuzzy neural networks for evaluating the creditworthiness of the borrowers. F. Abdulrahman, J. K. Panford and J. Hayfron [21] proposed a fuzzy logic approach to credit scoring for Micro Finance.

IV. THE PROPOSED MODEL ARCHITECTURE

The main objective of proposed model is to predict credit risk rating for Egyptian commercial banks in advance with a reasonable accuracy. The proposed model is a method of measuring the creditworthiness for commercial banks that shows whether commercial banks have a history of financial stability. This model is based on the quantitative financial indicators that are presented in Table 1. As shown in Fig.1, the proposed model consists of the following seven components:

1. Member function base
2. Fuzzy rule base
3. Fuzzy inference engine
4. Database Management System (DBMS)
5. Database (DB).
6. User interface
7. Defuzzification process

The main components of the proposed model are discussed briefly in the following subsections.

A. Membership Function Base

Membership function base is a mechanism that presents the membership functions of linguistic variables terms. This section presents membership functions for each financial indicator of the bank performance.

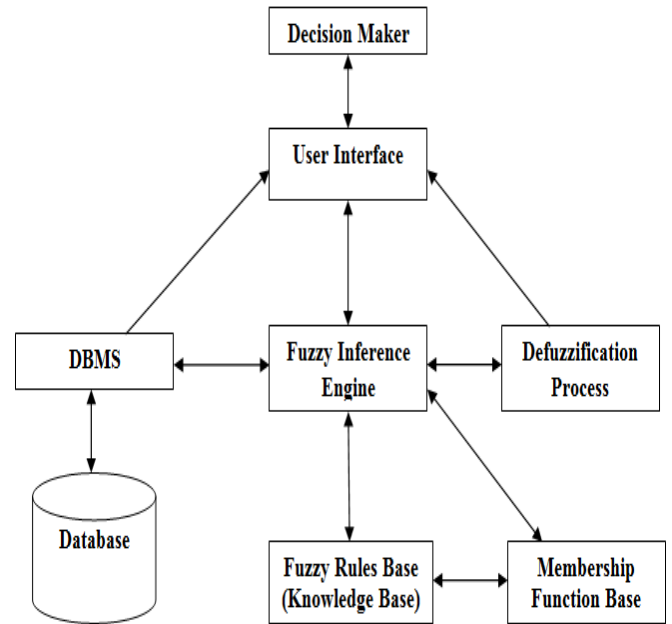


Figure1. The Proposed Model Architecture

1) *Profitability ratio*: Fuzzy logic techniques use linguistic variables in profitability evaluation to represent ROC indicator and NPM indicator. In this case, each indicator value is assigned a degree of membership in relation to the linguistic descriptors “high”, “medium”, and “low” as presented in Tables 3, 4 and Fig.2, 3.

a) Membership functions for ROC indicator:

TABLE 3. FUZZY VALUES FOR ROC

Linguistic	Notation	Numerical range
Low	L	[0 , 2.63]
Medium	M	[0.78 , 3.95]
High	H	[2.64 , 5.26]

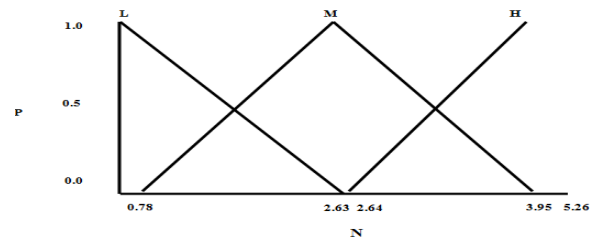


Figure 2. Membership functions for ROC

b) Membership functions for NPM indicator:

TABLE 4. FUZZY VALUES FOR NPM

Linguistic	Notation	Numerical range
Low	L	[0 , 43.08]
Medium	M	[12.92 , 64.62]
High	H	[43.09 , 86.16]

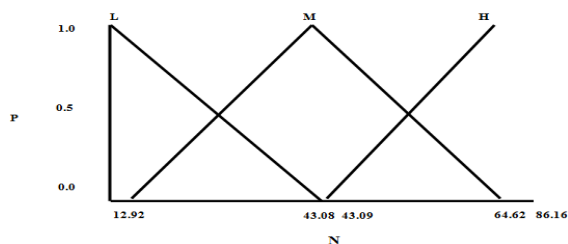


Figure 3. Membership Functions for NPM

2) *Debt-paying ability ratio*: Fuzzy logic techniques use linguistic variables in debt-paying ability evaluation to represent CTR indicator, QKR indicator, CYR indicator, and DTR indicator. In this case, each indicator value is assigned a degree of membership in relation to the linguistic descriptors “high”, “medium”, and “low” as presented in Tables 5, 6, 7, 8 and Fig. 4, 5, 6, 7.

a) *Membership functions for CTR indicator:*

TABLE 5. FUZZY VALUES FOR CTR

Linguistic	Notation	Numerical range
Low	L	[0 , 102.28]
Medium	M	[51.14 , 153.42]
High	H	[102.29 , 204.56]

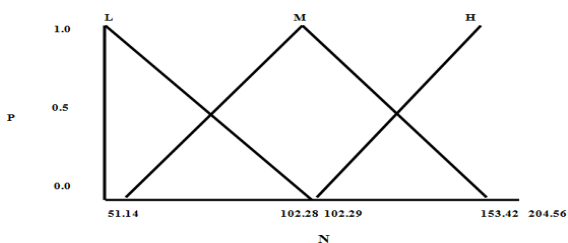


Figure 4. Membership Functions for CTR

b) *Membership functions for QKR indicator:*

TABLE 6. FUZZY VALUES FOR QKR

Linguistic	Notation	Numerical range
Low	L	[0 , 106.75]
Medium	M	[53.38 , 160.13]
High	H	[106.76 , 213.52]

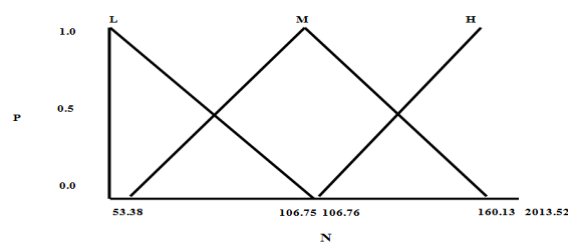


Figure 5. Membership Functions for QKR

c) *Membership functions for CYR indicator:*

TABLE 7. FUZZY VALUES FOR CYR

Linguistic	Notation	Numerical range
Low	L	[0 , 68.69]
Medium	M	[34.35 , 103.04]
High	H	[68.70 , 137.38]

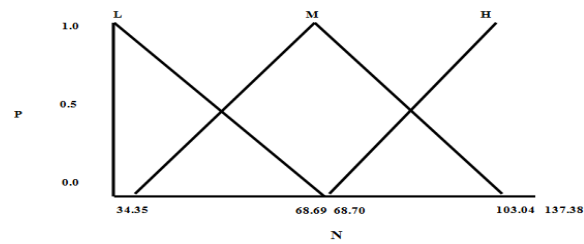


Figure 6. Membership Functions for CYR

d) *Membership functions for DTR indicator:*

TABLE 8. FUZZY VALUES FOR DTR

Linguistic	Notation	Numerical range
Low	L	[0 , 94.58]
Medium	M	[47.29 , 141.87]
High	H	[94.59 , 189.16]

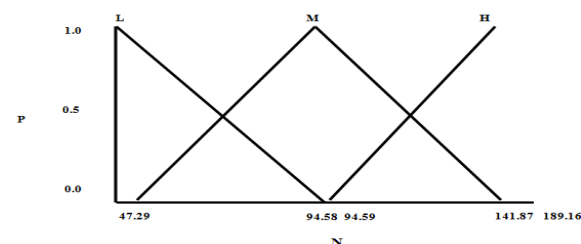


Fig. 7. Membership Functions for DTR

3) *Operation ability ratio*: Fuzzy logic techniques use linguistic variables in operation ability evaluation to represent TAT indicator. In this case, each indicator value is assigned a degree of membership in relation to the linguistic descriptors “high”, “medium”, and “low” as presented in Table 9 and Fig. 8.

a) *Membership functions for TAT indicator:*

TABLE 9. FUZZY VALUES FOR TAT

Linguistic	Notation	Numerical range
Low	L	[0 , 2.18]
Medium	M	[1.09 , 3.27]
High	H	[2.19 , 4.36]

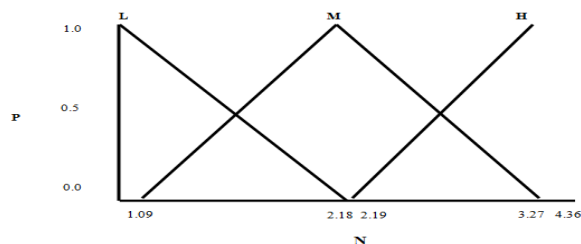


Figure 8. Membership Functions for TAT

4) *Liquidity ability ratio*: Fuzzy logic techniques use linguistic variables in liquidity evaluation to represent SA indicator, DA indicator, and LD indicator. In this case, each indicator value is assigned a degree of membership in relation to the linguistic descriptors “high”, “medium”, and “low” as presented in Tables 10, 11, 12, and Fig. 9, 10, 11.

a) Membership functions for SA indicator:

TABLE 10. FUZZY VALUES FOR SA

Linguistic	Notation	Numerical range
Low	L	[0 , 21.2]
Medium	M	[4.26 , 38.34]
High	H	[21.3 , 42.7]

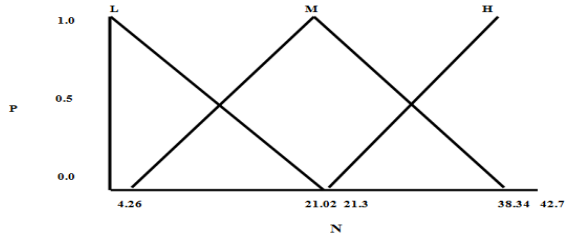


Figure 9. Membership Functions for SA

b) Membership functions for DA indicator:

TABLE 11. FUZZY VALUES FOR DA

Linguistic	Notation	Numerical range
Low	L	[0 , 70.6]
Medium	M	[14.5 , 127.8]
High	H	[70.8 , 141.6]

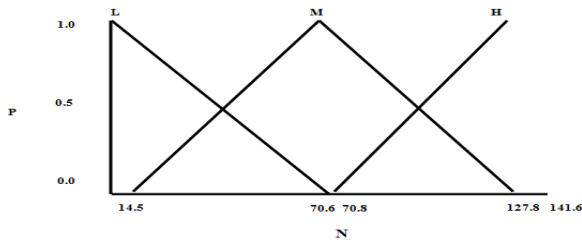


Figure 10. Membership Functions for DA

c) Membership functions for LD indicator:

TABLE 12. FUZZY VALUES FOR LD

Linguistic	Notation	Numerical range
Low	L	[0 , 49.9]
Medium	M	[13.3 , 90.3]
High	H	[50 , 100]

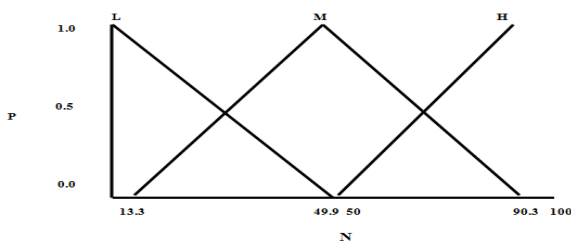


Figure 11. Membership Functions for LD

B. Fuzzy Rules Base

Fuzzy rules base contains the expert knowledge of indicators relations and the formation of a total judgment as if-then rules. All the fuzzy rules together compose the so called "knowledge base". The model allows for adding or updating theses rules in case of extending the rules base. Fuzzy rules are used to calculate financial ratios including

profitability, debt-paying ability, operation ability, and liquidity.

1) *Profitability ratio*: As shown in Table 13, this section presents samples of the profitability ratio rules that are applied by the fuzzy inference engine. Profitability ratio is based on calculating the following two indicators:

- $ROC = (\text{Net income} - \text{Dividends}) / (\text{Debt} + \text{Equity})$
- $NPM = \text{Net Profit} / \text{Total Revenue}$

TABLE 13. PROFITABILITY RATIO RULES SAMPLES

Rule #	Fuzzy Rule
1	IF ROC is low AND NPM is low THEN Profitability is low
2	IF ROC is low AND NPM is high THEN Profitability is medium
3	IF ROC is high AND NPM is medium THEN Profitability is high

2) *Debt-paying ability ratio*: As shown in Table 14, this section presents samples of the dept-paying ability ratio rules that are applied by the fuzzy inference engine. Dept-paying ability ratio is based on calculating the following four indicators:

- $CTR = \text{Current Assets} / \text{Current Liabilities}$
- $QKR = (\text{Current Asset} - \text{Inventories}) / \text{Current Liabilities}$
- $CYR = \text{Current Assets} / \text{Current Liabilities}$
- $DTR = \text{Total Debit} / \text{Total Assets}$

TABLE 14. DEPT-PAYING ABILITY RATIO RULES SAMPLES

Rule #	Fuzzy Rule
1	IF CTR is low AND QKR is low AND QKR is low AND DTR is low THEN Dept-Paying Ability is low
2	IF CTR is low AND QKR is medium AND QKR is medium AND DTR is high THEN Dept-Paying Ability is medium
3	IF CTR is low AND QKR is medium AND QKR is high AND DTR is low THEN Dept-Paying Ability is medium

3) *Operation ability ratio*: As shown in Table 15, this section presents samples of the operation ability ratio rules that are applied by the fuzzy inference engine. Operation ability ratio is based on calculating the following indicator:

- $TAT = \text{Sales or Revenues} / \text{Total Assets}$

TABLE 15. OPERATION ABILITY RATIO RULES SAMPLES

Rule #	Fuzzy Rule
1	IF TAT is low THEN Operation Ability is low
2	IF TAT is medium THEN Operation Ability is medium
3	IF TAT is high THEN Operation Ability is high

4) *Liquidity ratio*: As shown in Table 16, this section presents samples of the liquidity ratio rules that are applied by the fuzzy inference engine. Liquidity ratio is based on calculating the following three indicators:

- SA = Securities / Assets
- DA = Deposits / Assets
- LD = Loans / Deposits

TABLE 16. LIQUIDITY RATIO RULES SAMPLES

Rule #	Fuzzy Rule
1	IF SA is low AND DA is high AND LD is low THEN Liquidity is medium
2	IF SA is medium AND DA is low AND LD is low THEN Liquidity is low
3	IF SA is high AND DA is low AND MBGR is low THEN Liquidity is medium

C. Other Components

1) *Fuzzy Inference engine*: The most important two types of fuzzy inference method are Mamdani and Sugeno fuzzy inference methods [22]. This model is based on Mamdani inference method as the core of the reasoning process. The Mamdani-style fuzzy inference process is performed in four steps [23]:

1. Fuzzification of the input variables
2. Rule evaluation
3. Aggregation of the rule outputs
4. Defuzzification

The inputs of the model include the indicators values for the profitability, debt-paying ability, operation ability and liquidity ratios. The output includes fuzzy values and defuzzified values. The role of fuzzy inference engine is to match the fuzzy rules that are contained in the rules base with the entered values for the indicators data that is stored in the database to identify which rules should be applied and manage the reasoning process.

2) *DBMS*: The bank's data is managed by the database management system (DBMS). DBMS is used by the users to perform model's database managing operations including storing, retrieving, adding, deleting and modifying.

3) *Database (DB)*: Database is used to store the entire bank's data including the financial indicators data. It is managed by the DBMS that allows the users (decision makers) to add, update and delete the bank's data.

4) *User Interface (UI)*: User interface facilitates communication between the user (decision maker) and the implemented system of the model. It is also used to input the bank's data and show the results.

5) *Defuzzification Process*: Defuzzification is the process which transforms a fuzzy output of the inference engine to crisp output [24]. The input for the defuzzification process is the aggregate output fuzzy set and the output is a crisp number [25]. There are several defuzzification methods. Each provides a means to choose a single output based on the implied fuzzy sets [26]. Commonly used defuzzifying methods are:

- The mean of maximum method.
- The maximizing decision.
- The center of gravity method. [27]

In this paper, the center of gravity method is used as a defuzzification strategy.

V. THE ALGORITHM OF THE PROPOSED MODEL

This section presents an algorithm of the proposed model for determining and predicting the credit risk rating for Egyptian commercial banks. Fig.12 shows the flow chart of the proposed model.

1. Login into the system.
2. Input the values of indicators for each financial ratio used in the credit risk rating assessment.
3. Determine the membership function numerical range for each indicator linguistic value.
4. If new bank
{
 Input indicators values and data of the bank
}
Else
{
 Retrieve indicators values and data of the bank
}
5. Determine the bank indicator membership value.
6. Calculate the final value for each financial ratio by applying the appropriate fuzzy rules.
7. Defuzzify the calculated financial ratios values by using the center of gravity method.
8. Compare the output of the defuzzification process with Moody's ratings.
9. Print the class of credit risk rating of the bank.

VI. THE IMPLEMENTATION OF THE PROPOSED MODEL

This section presents the major steps used in implementing the proposed model and evaluating its effectiveness. The proposed model was implemented using fuzzy logic in MATLAB since it is the most common tool that is used for fuzzy systems. It can be used for defining the input, output, fuzzy rules, and the shape of membership function for the fuzzy system.

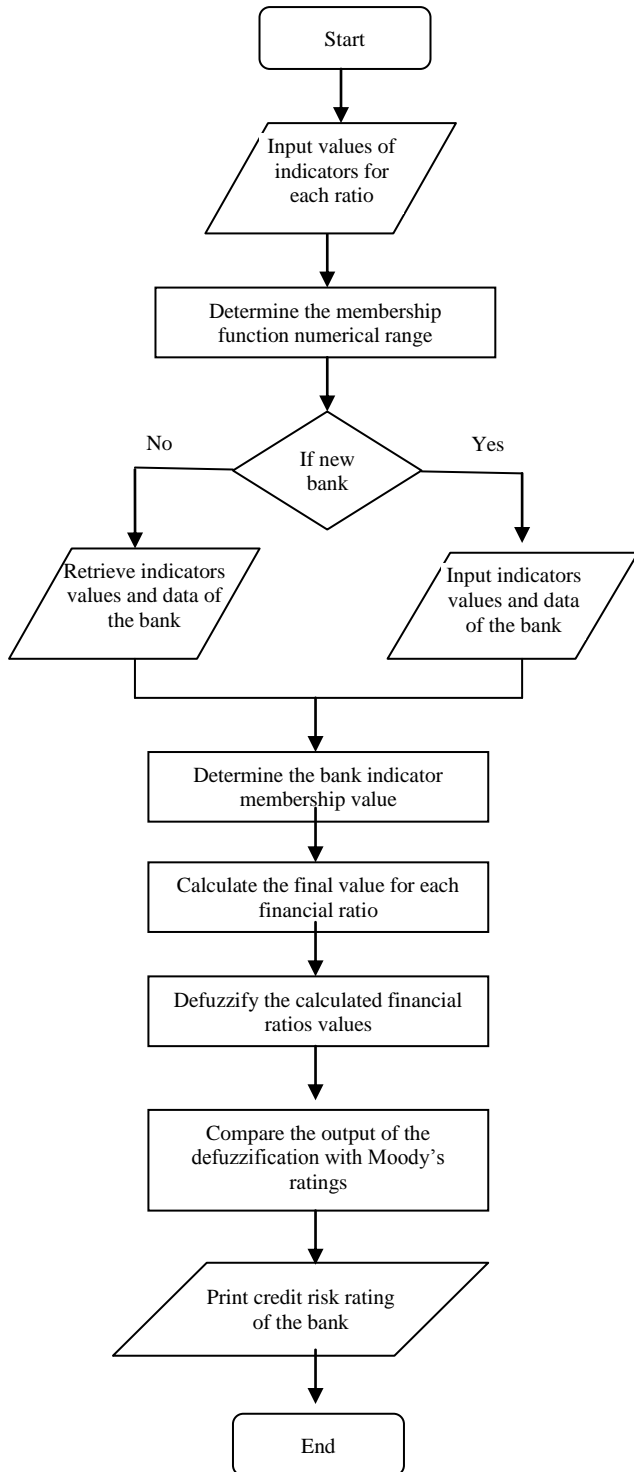


Figure 12 . Flow Chart of the Proposed Model

Using MATLAB, financial ratios membership functions were calculated, including profitability membership, debt-paying ability membership, operation ability membership and liquidity membership. The proposed model provides a user interface that allows decision makers to interact with it. The Visual Studio 2013 was used to create the graphical user interface (GUI) that allows decision makers to interact with electronic devices with images rather than text commands. The proposed model was applied on CIB Egyptian

commercial bank. The calculated ratios by the model for the CIB bank are as follows:

- Profitably ratio is low (2.60)
- Debt-paying ability ratio is low (41.99)
- Operation ability ratio is medium (9.86)
- Liquidity ratio is low (25.7)

Calculation of CIB Bank credit rating percentage:

$$f = \frac{(2.60 \times 25) + (41.99 \times 25) + (9.86 \times 50) + (25.7 \times 25)}{2.60 + 41.99 + 9.86 + 25.7}$$

$$f = \frac{65 + 1049.75 + 493 + 642.5}{80.15}$$

$$f = \frac{2250.25}{80.15} = 28.07$$

Percentage of CIB bank credit rating by defuzzification process is (28.07), based on profitably ratio is low (2.60), dept-paying ability ratio is low (41.99), operation ability ratio is medium (9.86) and liquidity ratio is low (25.7). As a result, the proposed model predicted the rating classification of the CIB bank according to Moody's ratings as (Ba3).

VII. CONCLUSION AND FUTURE WORK

The proposed model in this paper has proven its effectiveness in predicting the credit risk rating of the commercial banks in advance with a reasonable accuracy. This paper also provides a set of financial indicators which can be used in the assessment of the bank credit risk rating. These indicators were classified into four categories: profitability, debt-paying ability, operation ability and liquidity. By using the proposed model, decision makers will be able to determine the class of credit risk rating of commercial banks. The results showed that Fuzzy logic is one of the most significant techniques in machine learning that are used to predict credit risk rating of commercial banks. The results also indicated that fuzzy logic technique is more scalable, reliable, stable, and different from classical methods. It is recommended as a future work to integrate other machine learning techniques such as neural networks with the proposed model in order to enhance the accuracy of the model results.

REFERENCES

- [1] K., Christian, "Credit Rating and the Impact on Capital Structure. Norderstedt," *Germany: Druck und Bindung*, 2009.
- [2] L. J. White, "Credit Rating Agencies and the Financial Crisis: Less Regulation of CRAs Is a Better Response," *Journal of International Banking Law*, vol. 25, 2010.
- [3] N.S. Abdel Megeid, "The Impact of Effective Credit Risk Management on Commercial Banks Liquidity Performance: Case of Egypt," *International Journal of Accounting and Financial Management Research (IJAFMR)*, vol. 3, 2013.
- [4] J. Y. Yuan and L. Y. Guang, "Credit Risk Rating of China's Commercial Bank to SME Loans," *Chinese-Egyptian Research Journal*, vol. 2, pp. 9-33, 2013.

- [5] A. K. Abdelmoula, "Bank Credit Risk Analysis with k-nearest Neighbor Classifier: Case of Tunisian Banks," *Accounting and Management Information Systems*, vol. 14, no. 1, pp. 79-106, 2015.
- [6] Moody's Ratings Definitions. [Online]. Available: <https://www.moodys.com/Pages/amr002002.aspx>, [Jan. 21, 2016].
- [7] L. A. Zadeh, "Fuzzy Logic, Neural Networks, and Soft Computing," *Communications of the ACM*, vol. 37, pp. 77-84, 1994.
- [8] L. A. Zadeh, "Fuzzy Sets," *Information and Control*, vol. 8, pp. 338-353, 1965.
- [9] L.A. Zadeh, "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes," *IEEE Trans*, vol. 1, pp. 28-44, 1973.
- [10] L. Yijun, C. Qiuru, L. Ye and Q. Jin, "Artificial Neural Networks for Corporation Credit Rating Analysis," *IEEE*, vol. 1, pp. 81-84, 2009.
- [11] H. A. Abdou, "Genetic Programming for Credit Scoring: The Case of Egyptian Public Sector Banks," *Expert Systems with Applications*, vol. 36, pp. 11402-11417, 2009.
- [12] W. Hongxia, L. Xueqin and L. Yanhui, "Enterprise Credit Rating Model Based on Fuzzy Clustering and Decision Tree," *Information Science and Engineering*, pp. 105 – 108, 2010.
- [13] C. Tsai and M. Chen, "Credit rating by hybrid machine learning techniques" *Applied Soft Computing*, vol. 10, pp. 374-380, 2010.
- [14] Y. Wei, S. Xu, F. Meng, "The Listed Company's Credit Rating Based on Logistic Regression Model Add Non-financial Factors," in *2nd Int. Conf. Modeling, Simulation and Visualization Methods*, 2010, pp. 172 – 175.
- [15] P. Hájek, "Municipal Credit Rating Modeling by Neural Networks," *Decision Support Systems*, vol. 51, pp. 108-118, 2011.
- [16] V. H. Duc and N. D. Thien, "A New Approach to Determining Credit Rating & Its Applications to Vietnam's Listed Firms," *Open University, Ho Chi Minh City, Vietnam*, 2013.
- [17] M. F. Rafiei, S. M. Manzari and M. Khashei, "An ANN Based New Approach Credit Rating Prediction Model: Evidence from Tehran Stock Exchange," *International Journal of Computer Science and Artificial Intelligence*, vol. 3, pp. 143-153, 2013.
- [18] M. R. Gholamian, S. Jahanpour and S. Mahdi Sadatrasoul, "A New Method for Clustering in Credit Scoring Problems," *Journal of mathematics and computer Science*, vol. 6, pp. 97-106, 2013.
- [19] R. H. Abiyev, "Credit Rating Using Type-2 Fuzzy Neural Networks," *Mathematical Problems in Engineering*, pp. 8-16, 2014.
- [20] N. Shovgun, "Fuzzy Neural Networks for Evaluating the Creditworthiness of the Borrowers," *International Journal Information Theories and Applications*, vol. 21, pp. 54-59, 2014.
- [21] U. F. Abdulrahman, J. K. Panford and j. Hayfron-Acquah, "Fuzzy Logic Approach to Credit Scoring for Micro Finances in Ghana," *International Journal of Computer Applications*, vol. 94, pp. 11-18, 2014.
- [22] S.N. Sivanandam, S. Sumathi and S. N. Deepa, *Introduction to Fuzzy Logic using MATLAB*. Springer-Verlag, 2007.
- [23] G. Andrew, I. Belik and S. Rahimi1, "A Hybrid Expert System for IT Security Risk Assessment" in *Int. Conf. Parallel and distributed Processing Techniques and Applications*, 2010.
- [24] Atef T. Raslan, Nagy. R. Darwish and Hesham A. Hefny, "Towards a Fuzzy based Framework for Effort Estimation in Agile Software Development," *International Journal of Computer Science and Information Security*, vol. 13, no. 1, 2015.
- [25] A. A. Mohamed and A. A. Salama, "A Fuzzy Logic Based Model for Predicting Commercial Banks Financial Failure," *International Journal of Computer Applications*, vol. 79, no. 11, 2013.
- [26] W. S. Levine, *The Control Handbook*. CRC Press, 1996.
- [27] S. Naaz1, A. Alam and R. Biswas, "Effect of Different Defuzzification Methods in a Fuzzy Based Load Balancing Application," *IJCSI International Journal of Computer Science Issues*, vol. 8, no 1, 2011.

Performance Evaluation of Sigmoid loss for Functional and Geometric Margin Based MCE in Robust Speech Recognition

Syed Abbas Ali

Dept. of Computer & Information Systems Engineering,
N.E.D University of Engineering & Technology,
Karachi, Pakistan

Adiba Jafar

Dept. of Computer Systems Engineering,
Usman Institute of Technology,
Karachi, Pakistan

Abeer Javed Syed

Dept. of Computer Systems Engineering,
Sir Syed University of Engineering & Technology
Karachi, Pakistan

Kamran Khanzada

University of Karachi
Karachi, Pakistan

Abstract—This paper presents demonstrative experiments to evaluate the performance of sigmoid loss function in term of percentage error for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in the presence of three presence of three different noises (White, Pink, and Brown) with SVM classifiers using recorded and pre-conditioned speech data samples. The experimental framework consists of TI-Digit corpus and recorded digits taken from real environment with conventional and geometric SVM classifier in the presence of three different types of noises taken from NOISEX-92 noise-in-speech database. Experimental results demonstrated that average percentage error values of sigmoid loss function in GM-MCE is substantially less in comparison with percentage error values of FM-MCE for all isolated TI-Digit and recorded digit (0-9). Whereas, noise tolerance capability of GM-MCE based sigmoid loss function is considerably better than conventional FM-MCE based sigmoid loss function.

Keywords—component; Statistical Learning, Margin Based Learning, Functional Margin, Geometric Margin, Automatic Speech Recognition.

I. INTRODUCTION

Discriminative learning criterions are used to train a Hidden Markov Model (HMM) [1,2] to enhance the generalization capability of the acoustic model. From the statistical learning theory point of view [3], increase in the margin reflects improvement in generalization capability. Conventional discriminative learning criterions and soft margin estimation based discriminative learning focuses on empirical risk minimization and improving the margin respectively. Among others Discriminative criterions, Minimum classification error (MCE) [4] shows considerable improvement to enhance the generalization ability of acoustic model in speech recognition applications. Soft margin based discriminative training criterion [5] does not perform well with noisy data samples due to hinge loss used in SVM as loss function to improve

recognition performance. Whereas, sigmoid loss function shows significant performance in comparison with hinge loss function with and without SVM classifiers in the presence of noise [43]. The limitation of soft margin estimation framework due to hinge loss function is addressed in [6] by introducing new optimized objective function of soft margin estimation (SME) based on separation measures (sigmoid loss) using Geometric margin Minimum Classification Error (MCE) criteria in soft margin estimation framework.

In this paper, demonstrative experiments have been presented to evaluate the performance of sigmoid loss function in the presence of white noise, pink noise and brown noise for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in term of percentage error. Rest of the paper is organized as follow. The consequent section provides related works with addressing the issues in margin based learning framework. Section III provides the mathematical framework for functional margin based MCE criterion. The formulation of geometric margin based MCE is presented in section IV. Experimental results of sigmoid loss function for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in the presence of noise is presented in section V. Finally, conclusions are drawn in section IV.

II. RELATED WORK

Maximum likelihood estimation (MLE) [7,8,9] is considered as a generative model or non-discriminative learning approach, which is focused on data distribution modeling instead of directly classifying class boundaries. In contrast, discriminative learning approach discriminately learns the parameters of joint probability model to minimize the recognition/classification error [10]. The objective of discriminative training (DT) is to introduce a discriminative criterion to the training method of Hidden Markov Models (HMMs). Several discriminative training methods have been proposed for ASR, such as maximum mutual information estimation (MMIE) [11,12,13], minimum classification error

(MCE) [14,15]; and minimum word/phone error (MWE/MPE) [16,17]. Despite significant progress in discriminative training methods of speech recognition, most of the unsolved issues related to discriminative training are still under consideration of the speech research community. For HMM based speech recognition, conventional discriminative training criteria directly minimize the empirical risk on the training data sample but do not focus on the model generalization. In other words, the aim of discriminative training criteria is to minimize the classification error on training sample as model estimation but do not show any significant performance to improve the generalization capability of acoustic model for new unseen test data samples [18]. The generalization capability is an ability to translate gains in the training dataset to test dataset. Yu et al[19] used discriminative training to achieve generalization capability by optimizing the smoothed empirical error rate on training data samples. Recently, many researches have been reported to incorporate margins (distance between the decision boundary and well classified data samples) into discriminative training method [20,21,22,23,24,25] to further enhance the generalization capability. Support vector machine (SVM) [26] based on statistical learning theory have demonstrated significant progress in enhancing the generalization capabilities as compared to any other conventional discriminative classifiers. Recent work shows that Support vector machine (SVM) has achieved great success in a variety of application in the field of speech recognition and in some research works related to application of SVM in acoustic modeling tasks in which ASR researchers made direct use of standard SVM formulation in isolated speech recognition task, such as, digit recognition [27], phoneme recognition [28], and speaker recognition and verification [29], etc. Due to complex speech dynamic, the speech patterns are not linearly separable, and one of the prominent issues of SVM is to select an appropriate kernel to map speech patterns into a high dimensional space to make it suitable for linear classification. Different kernels have been reported in the literature for speech patterns [30,31,32]. Some other technologies of SVMs were reported regarding loose coupling of SVM with HMM [33] and combination of SVM and HMM, called HM-SVM [34] with discrete distribution. The main focus of HM-SVM was to find the optimal projection matrix, while the loose coupling of SVM with HMM facing the generalization issue with a larger margin due to dynamic nature of the speech patterns which lead the technical problems in terms of training and recognition complexity. Large margin estimation (LME) and its variant large relative margin estimation (LRME) of HMMs have been proposed with the concept of enhancing separation margin [35]. The main crux of the LME is that only correctly classified data samples take part in update models whereas, it is important to note that misclassified data samples are also substantial for classifier learning. To address this problem in LME, Soft margin estimation (SME) was proposed by J.Li et al [5] from Georgia Tech University based on the idea of soft margin in support vector machines [26] to enhance the generalization capability of the learning classifiers. In contrast with LME, SME makes use of both misclassified and correctly classified data samples to update models and the performance of the SME can be improved when the distribution of testing and training data samples become quite comparable[36]. SME

does not show significant results with noisy speech recognition which increases the mismatch between training and testing data samples. Demonstrative experiment has been presented in [43] to evaluate the performance of hinge loss used as loss function in soft margin estimation (SME) in comparison with other loss functions (Logistic, Savage, Sigmoid) and concluded that sigmoid loss function perform well for all prescribed conditions. Addressing the inefficiency of functional margin, new version of minimum error classification (MCE) has been introduced by replacing separation measure of functional margin with geometric margin [37,38]. Extended the observation obtained from soft margin based learning, soft margin based new optimized objective function for ASR was presented in [6] by placing the Geometric Margin based (LGM-MCE) in place of Functional Margin MCE separation (misclassification) measure.

III. FORMULATION OF FUNCTIONAL MARGIN BASED MCE CRITERION

The main objective of minimum classification error is to reduce the total error counts in training data samples and loss function minimization [15]. The main goal of MCE training is to correctly discriminate the observation O for recognition results rather than to fit the distribution to data. In MCE, a misclassification measure is used to distinguish the competing class from the true class [14] can be defined as;

$$d(O_t, \Lambda) = -g_t(O_t, \Lambda) + \log \left[\frac{1}{N-1} \sum_{y, y \neq t} \exp g_y(O_t, \Lambda) \right]^{1/\eta} \quad (1)$$

In conventional MCE formulation, the misclassification suggested in [83],

$$d(O_t, \Lambda) = -g_t(O_t, \Lambda) + \log [\sum_{\hat{W}_t \neq W_t} P(O_t | \hat{W}_t) \cdot P(\hat{W}_t)] \quad (2)$$

where

$$g_t(O_t, \Lambda) = \log P(O_t | W_t) = \log [P(O_t | W_t) \cdot P(W_t)] \quad (3)$$

Now put values of (3) in (2) to get the equation of separation (misclassification) measure;

$$d(O_t, \Lambda) = -\log [P(O_t | W_t) \cdot P(W_t)] + \log [\sum_{\hat{W}_t \neq W_t} P(O_t | \hat{W}_t) \cdot P(\hat{W}_t)] \quad (4)$$

Misclassification measure in (4) is a continuous function of acoustic model parameter λ and tries to emulate decision rule for the observation vectors O , if $d(O_t, \lambda) \leq 0$ implies correct decision while $d(O_t, \lambda) > 0$ means wrong decision or misclassification. To obtain the smoothed error count for O_t , the misclassification measure is introduced into sigmoid function as,

$$\ell_t(O, \Lambda) = \ell[d(O_t, \Lambda)] \quad (5)$$

ℓ is a sigmoid loss function,

$$\ell[d(O_t, \Lambda)] = \frac{1}{1 + \exp(-\gamma d(O_t, \Lambda) + \theta)} \quad (6)$$

By setting the values of θ as zero and γ is greater than 1, the value of misclassification measure $d(O_t, \Lambda)$ is less than zero

implies correct decision. The objective of MCE is to reduce the total smothered error over entire training data samples. The MCE criterion can be written as:

$$\Lambda_{MCE} = \arg \min_A \sum_{t=1}^T \ell_t[d(O_t, \Lambda)] \quad (7)$$

The optimized objective function of MCE is represented as;

$$\Lambda_{MCE} = \arg \min_A \frac{1}{N} \sum_{t=1}^T \frac{1}{1 + \exp(-\gamma d(O_t, \Lambda) + \theta)} \quad (8)$$

The equation of separation measure for minimum classification error can be represented as in [39];

$$\frac{P(O_t|W_t) \cdot P(W_t)}{\sum_{\hat{W}_t} P(O_t|\hat{W}_t) \cdot P(\hat{W}_t)} \quad (9)$$

Soft margin estimation (SME) can be estimated by combining the two optimized function in one objective function [5];

$$\Lambda_{SME} = \frac{\lambda}{\rho} + \frac{1}{N} \sum_{t=1}^N (\rho - d(O_t, \Lambda)) \Gamma(O_t \in U) \quad (10)$$

Introducing the value of Eq. (9) in equation (10), the functional margin based MCE criterion can be defined as;

$$\Lambda_{SME} = \frac{\lambda}{\rho} + \frac{1}{N} \sum_{t=1}^N (\rho - \frac{P(O_t|W_t) \cdot P(W_t)}{\sum_{\hat{W}_t} P(O_t|\hat{W}_t) \cdot P(\hat{W}_t)}) \Gamma(O_t \in U) \quad (11)$$

IV. FORMULATION OF GEOMETRIC MARGIN BASED MCE

Geometric margin in Minimum error classification framework formulation for general class of discriminant functions is well established in [13,14]. In geometric margin formulation for ASR, the Euclidean distance is defined in term of separation measure \hat{r} [6];

$$\hat{r} = \frac{|d(O_t, \Lambda) + o(f)|}{\|\nabla_{O_t} d(O_t, \Lambda)\|} \quad (12)$$

Eq.(12) defining the incremental changes in geometric margin by decreasing the norm of gradient of the separation measure and improving the functional margin in the area of class decision boundary. The equation of LGM-MCE method based separation measure can be written as;

$$\mathcal{D}(O_t, \Lambda) = \frac{d(O_t, \Lambda)}{\|\nabla_{O_t} d(O_t, \Lambda)\|}, \quad (13)$$

Introducing the Eq. (13) in (10), new optimize objective function of soft margin estimation (SME) corresponding to Large Geometric Margin MCE (LGM-MCE) training criterion can be obtained;

$$\Lambda_{SME} = \frac{\lambda}{\rho} + \frac{1}{N} \sum_{t=1}^N (\rho - \mathcal{D}(O_t, \Lambda)) f(O_t \in \hat{U}) \quad (14)$$

Substituting the equation of separation measure for minimum classification error (9) in (13), equation of Geometric Margin based separation measure in term of Functional Margin MCE can be obtained for ASR. Eq. (14) provides soft margin based mathematical framework for ASR with Large Geometric Margin based MCE (LGM-MCE) criterion.

V. EXPERIMENTAL RESULTS AND DISCUSSION

Demonstrative experiments have been presented to evaluate the performance of sigmoid loss function in term of percentage error for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in the presence of three different noises (White, Pink, and Brown) with SVM classifiers using recorded and pre-conditioned speech data samples. Demonstrative experiments consists of TI-Digit corpus [41] and recorded digits taken from real environment with conventional and geometric SVM classifier in the presence of three different types of noises taken from NOISEX-92 noise-in-speech database [40,42]. The experimental methodology comprises on TI-digits (0-9) standard isolated digit database and digits recorded from real environment. Standard ITU recommendations have been adopted for speech corpora development using Microsoft Windows 7 built-in sound recorder to record the 10 utterances from speaker of each digit (0-9). We made use of specified configuration of Microsoft Windows 7 built-in sound recorder input digits 0 to digit 9 were recorded in noise free environment. Afterwards, Audacity software was used to add white noise, brown noise and pink noise in both data sets. A number of experiments were performed with the evaluation of cepstrum coefficient values for each digit in clean and noisy conditions to evaluate the percentage improvement of GM-MCE based sigmoid loss function in comparison with FM-MCE sigmoid loss function. Experimental framework was based on several pieces of code for both conventional MCE and geometric MCE implemented and observed in MATLAB tool version 10.0. To determine the peak value of cepstrum coefficient, cepstrum of each digit (0-9) were obtained with and without noise to differentiate noisy data sample from clean digit.

Based on the preliminaries observations, Table I. and Table II. summarized the experimental results comparing the percentage error values of sigmoid loss function for both GM-MCE based sigmoid loss function and FM-MCE based sigmoid loss function with isolated TI-DIGIT and recorded data samples respectively.

TABLE I. PERCENTAGE ERROR VALUES OF SIGMOID LOSS FUNCTION WITH SVM CLASSIFIERS FOR TI-DIGIT

Digit	Conventional FM-MCE			GM-MCE		
	White	Pink	Brown	White	Pink	Brown
0	6.96	7.22	7.21	5.71	5.66	6.23
1	6.14	6.48	6.39	7.47	6.28	5.51
2	6.97	7.25	7.31	5.86	8.45	7.08
3	7.24	7.61	7.75	6.02	8.61	7.52
4	6.14	6.31	5.95	4.34	5.62	6.93
5	6.56	6.71	6.43	7.81	6.02	7.02
6	7.42	7.66	7.15	6.02	5.86	6.94
7	6.35	6.64	6.41	4.99	7.62	7.07
8	6.79	6.58	6.87	7.93	8.43	6.27
9	7.32	7.03	6.16	6.76	6.05	7.36

Sigmoid loss function comparative analysis has been performed in the presence of white noise, pink noise and brown noise between FM-MCE and GM-MCE with SVM classifier using Isolated TI-Digit and recorded digit taken from

environment. The bar graphs in Table III., and Table IV., provide the error difference between true function for all isolated TI-digit (0-9) and recorded digit in terms of percentage error. Experimental results interpretation is demonstrated using red bar, green bar, purple bar, blue bar, orange bar and sky blue bar for FM-MCE (white noise), FM-MCE (pink noise), FM-MCE (brown noise), GM-MCE (white noise), GM-MCE (pink noise) and GM-MCE (brown noise) respectively.

TABLE II. PERCENTAGE ERROR VALUES OF SIGMOID LOSS FUNCTION WITH SVM CLASSIFIERS FOR RECORDED DIGIT

Digit	Conventional FM-MCE			GM-MCE		
	White	Pink	Brown	White	Pink	Brown
0	7.21	7.26	7.15	5.87	6.31	6.79
1	6.52	6.56	6.81	5.83	5.88	7.75
2	6.71	6.61	6.51	7.27	5.74	5.92
3	7.04	7.35	7.06	5.94	9.15	6.84
4	7.12	7.05	7.21	6.73	7.63	6.99
5	6.34	6.08	6.53	6.09	5.12	7.52
6	6.62	7.44	6.72	8.12	6.44	7.92
7	6.95	7.85	6.89	6.05	7.62	7.85
8	7.56	7.37	7.62	8.25	8.87	7.37
9	6.51	6.68	6.83	7.82	6.33	6.58

In Table III. GM-MCE based sigmoid loss function in white noise represent small percentage error values in comparison with conventional FM-MCE based sigmoid loss but some anomalies is observed with digits 1, digit 5 and digit 8. Similarly, GM-MCE based sigmoid loss provide small error values with pink and brown noise but some inconsistencies with digit 2, 3, 7, 8 and digit 4, 5, 7, 9 is observed respectively.

Table IV. GM-MCE based sigmoid loss function is perform well as compared to conventional FM-MCE based sigmoid loss function in white noise, but some variations is observed with digit 2, 6, 8, 9. Whereas, some irregularities is observed with conventional FM-MCE based sigmoid loss in comparison with proposed GM-MCE based sigmoid loss in pink and brown noise for digit 3, 4, 8 and digit 1, 5, 6, 7 respectively.

TABLE III. SIGMOID LOSS FUNCTIONS OF FM-MCE AND GM-MCE FOR TI-DIGIT (0-9)

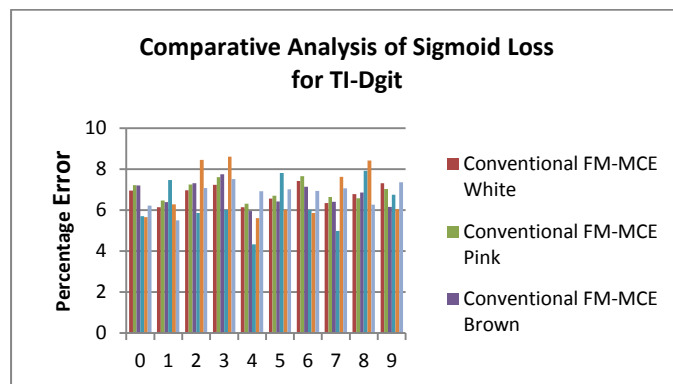


TABLE IV. SIGMOID LOSS FUNCTIONS OF FM-MCE AND GM-MCE FOR RECORDED-DIGIT (0-9)

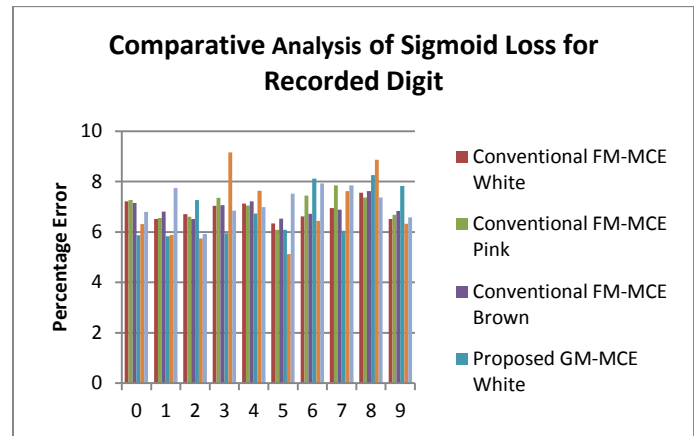


TABLE V. DIFFERENCE OF THE PERCENTAGE ERROR VALUES WITH ISOLATED TI-DIGIT AND RECORDED DIGIT FOR FM-MCE AND GM-MCE

Digit	Isolated TI-Digit			Recorded Digit		
	White	Pink	Brown	White	Pink	Brown
0	1.25	1.56	0.98	1.34	0.95	0.36
1	1.33	0.2	0.88	0.69	0.68	0.94
2	1.11	1.2	0.23	0.56	0.77	0.59
3	1.22	1	0.23	1.1	1.8	0.22
4	1.8	0.69	0.98	0.39	0.58	0.22
5	1.25	0.69	0.59	1.22	0.96	0.99
6	1.4	1.8	0.56	1.5	1	1.2
7	1.36	0.98	0.66	0.9	0.23	0.96
8	1.14	1.85	0.31	0.69	1.5	0.25
9	0.56	0.98	1.2	1.31	0.35	0.25

Table V. shows the percentage improvement of individual TI-Digit (0-9) and Recorded digit based on the difference of percentage error values of **FM-MCE** and **GM-MCE** in the presence of noise using red and black values respectively. Based on the difference of percentage error values of **FM-MCE** and **GM-MCE**, the percentage improvement of the **GM-MCE** over **FM-MCE** is calculated in the presence noise as shown in Table VI.

TABLE VI. PERCENTAGE IMPROVEMENT OF GM-MCE FOR ISOLATED TI-DIGIT AND RECORDED DIGIT

% Improvement	White	Pink	Brown
GM-MCE (TI-Digit)	1.24%	0.98%	0.53%
GM-MCE (Recorded)	0.94%	0.70%	0.26%

Based on the preliminaries results obtained from demonstrative experiments, average percentage error values of sigmoid loss function in GM-MCE is substantially less in comparison with percentage error values of FM-MCE for all isolated TI-Digit and recorded digit (0-9). The percentage improvement of the GM-MCE over FM-MCE with white, pink

and brown noises for Isolated TI-Digit and Recorded digit as shown in Table VI., are 1.24%, 0.98%, 0.53% and 0.94%, 0.70 and 0.26% respectively. Demonstrative experimental results indicate that noise tolerance capability of GM-MCE based sigmoid loss function is considerably better than conventional FM-MCE based sigmoid loss function

VI. CONCLUSION

This paper evaluated the performance of sigmoid loss function for Functional margin MCE (FM-MCE) and Geometric margin MCE (GM-MCE) in term of percentage error with white noise, pink noise, and brown noise on recorded and pre-conditioned utterances using SVM classifier. Demonstrative experiments have been implemented and observed in MATLAB tool version 10.0 to estimate the error values of sigmoid loss function in the presence of noise with SVM classifier. Experimental results show that GM-MCE has considerably less percentage error values as compared to conventional FM-MCE. The percentage improvement of the GM-MCE over FM-MCE with white, pink and brown noises for Isolated TI-Digit and Recorded digit are 1.24%, 0.98%, 0.53% and 0.94%, 0.70% and 0.26% respectively, which show GM-MCE has considerably better noise tolerance capability over FM-MCE.

References

- [1] L.R.Rabiner, "A tutorial on hidden markov models and selected applications in speech recognition," In Proc. IEEE, vol.77, pp.257-286,1989.
- [2] L.R.Rabiner and B.-H. Juang "An introduction to hidden markov models," IEEE Trans. On Acoustic, Speech and Signal processing, vol.3, no.1, pp. 4-16, 1986.
- [3] O. Bousquet, S. Bouchern and G. Lugosi, "Introduction to statistical learning theory. Advanced lectures on machine learning lecture notes in artificial intelligence 3176, Eds. Heidelberg, Germany: Springer, 2004, pp.167-207.
- [4] R.Schlueter, W.Macherey, B.Muller, and H.Ney "Comparison of discriminative training criteria and optimization methods for speech recognition," Speech Communication, vol.34, pp.287-310, 2001.
- [5] J. Li and C. -H. Lee, "Soft margin feature extraction for automatic speech recognition", Proc. Interspeech, 2007.
- [6] S.A. Ali and N.G. Haider, "Margin Based Learning Framework with Geometric Margin Minimum Classification Error for Robust Speech Recognition," International Journal of Sciences: Basic and Applied Research (IJSBAR), vol.11, pp. 39-48, 2013
- [7] A.P. Dempster, N. M. Laird and D. B. Gopinath, "Maximum Likelihood from incomplete data via the EM algorithm," J. Roy.Stat.Soc., vol.39, pp.1-38, 1977.
- [8] L.R.Liporace, "Maximum likelihood estimation for multivariate observations of Markov sources," IEEE Trans. on Information Theory, vol.22, pp.729-734, 1982.
- [9] S.M. Kay, Fundamental of statistical signal processing I: Detection Theory. Englewood Cliffs, NJ: Prentice Hall, 1993.
- [10] X. He and L. Deng, Discriminative Learning for Speech Recognition: Theory and Practice, Morgan & Claypool, 2008.
- [11] Y. Normandin, "Maximum Mutual Information Estimation of Hidden Markov Models," In Automatic Speech and Speaker Recognition, edited by C.H.Lee, F.K.Soong and K.K.Paliwal, Eds. Kluwer Academics Publishers Norwell: M.A, 1996, pp.1-159.
- [12] L.R.Bahl, P.F.Brown, P.V.Desouza and R.L. Mercer, "Maximum Mutual Information Estimation of Hidden Markov Models parameters for speech recognition," In Proc. ICASSP, vol.1, pp. 49-52, 1986.
- [13] V.Valtchev, J.Odell, P. Woodland and S. Young, "Maximum Mutual Information Estimation training for large vocabulary recognition systems," Speech Communication, vol.22, pp. 303-314, 1997.
- [14] B. -H. Juang, W. Chou, and C.-H. Lee, "Minimum Classification Error rate methods for speech recognition," IEEE Trans. on Speech and Audio Proc. vol.5, pp.257-265, 1997.
- [15] B.-H. Juang, and S. Katagiri, "Discriminative learning for Minimum Error Classification," IEEE Trans. on Signal Processing, vol.40, pp.3043-3054, 1992.
- [16] D.Povey and P. Woodland, "Minimum Phone error and I-smoothing for improved discriminative training," In Proc. ICCASP, vol.1, pp. 105-108, 2002.
- [17] D. Povey, Discriminative training for large vocabulary speech recognition, Ph.D. dissertation, Cambridge University, Dept. Eng., Cambridge, UK, 2004.
- [18] H.Jiang, X. Li and C. Liu, "Large Margin Hidden Markov models for speech recognition," IEEE Trans. on Audio, Speech and Language Processing, vol.14, pp.1584-1595, 2006.
- [19] D.Yu, L.Deng, X.He and A.Acero, "Large Margin minimum classification training for Large-Scale Speech Recognition Tasks," In Proc. ICASSP, 2007.
- [20] H. Jiang and X. Li, "Solving large margin HMMs estimation via semi-definite programming," In Proc. ICASSP, vol.4, pp.IV-629-IV-632, 2007.
- [21] J. Li, M.Yuan and C.-H.Lee, "Soft margin estimation of Hidden Markov Model parameters," In Proc. Interspeech, pp.2422-2425, 2006.
- [22] X. Li, and H.Jiang, "A constrained joint optimization methods for large margin HMM estimation," In Proc. ASRU Workshop, pp.151-156, 2005.
- [23] C. Liu, H.Jiang and L.Rigazio, "Recent improvement of minimum relative margin estimation of HMMs for speech recognition," In Proc. ICASSP, vol.1, pp.269-272, 2006.
- [24] F.Sha, and L.Saul, "Large-Margin Gaussian mixture modeling for phonetic classification and recognition," In Proc. ICASSP, vol.1, pp.265-268, 2006.
- [25] D.Yu, L.Deng, X.He and A.Acero, "Use of incrementally regulated discriminative margins in MCE training for speech recognition," InProc. Interspeech, pp. 2418-2421, 2006.
- [26] C. Burges, "A tutorial on support Vector machine for pattern recognition," Data Mining and Knowledge Discovery, vol.2, pp.121-167, 1998.
- [27] I.Bazzi and D.Katabi, "Using SVM for spoken digit recognition," In Proc. International conference on spoken language processing, Beijing, China, 2000.
- [28] P. Clarkson and P.J.Moreno, "On the use of SVM for phonetic classification," In Proc. IEEE International conference on Acoustic, Speech, Signal Processing, pp.585-588, 1999.
- [29] V.Wan and W.M.Campbell, "SVM for speaker verification and identification," In Proc. Neural Networks for signal Processing X, pp.775-784, 2000.
- [30] W.Campbell, "Generalized linear discriminant sequence kernel for speaker recognition," In Proc. ICASSP, pp.161-164, 2002.
- [31] N.Smith and M.Niranjan, "Data dependent kernels in SVM classification of speech signals," In Proc. International conference on spoken language processing, Beijing, China, 2000.
- [32] N.Smith and M.F.Gales, "Speech recognition using SVMs," In Proc. 15th International Conference on Neural Information Processing Systems, pp.1197-1204, 2001.
- [33] J.Stadermann and G.Rigoll, "A hybrid SVM/HMM acoustic modeling approach to automatic speech recognition," In Proc. Interspeech, pp.661-664, 2004.
- [34] Y.Altun, I.Tsochantaridis and T.Hofmann, "Hidden Markov support vector machines," In Proc. ICML, pp.3-10, 2003.
- [35] C.Liu, H.Jiang and X.Li "Discriminative training of CDHMMs for maximum relative separation margin," In Proc. ICASSP, pp.1101-1104, 2005.

- [36] R.K.Aggarwal and M.Dave, "Acoustic modeling problem for ASR system: advances and refinements (Part II)," *International Journal of Speech Technology*, Springer, pp.309-320, 2011.
- [37] H. Watanabe, S. Katagiri, K. Yamada, E. McDermott, A. Nakamura, S. Watanabe, M. Ohsaki. " Minimum error classification with geometric margin control, " in *Proc. IEEE*, pp. 2170–2173. 2010.
- [38] H. Watanabe and S. Katagiri."Minimum classification error training with geometric margin enhancement for robust pattern recognition," in *Proc. IEEE MLSP (CD version)*, 1–6. 2011.
- [39] X.He, L.Deng, and W.Chou. "Discriminative Learning in sequential pattern recognition: A unified view for optimization-based speech recognition." *IEEE Signal Processing Magazine*, pp. 14-36, 2008.
- [40] A.P. Varga, H.J.M Steeneken, M. Tomlinson, and D.Jones, "The NOISEX-92 Study on the Effect of Additive Noise on Automatic Speech Recognition," In *Technical Report*, DRA Speech Research Unit,1992.
- [41] D.Ellis, "Clean Digits". Available:
<http://www.ee.columbia.edu/~dpwe/sounds/tidigits/>
- [42] [Spib.rice.edu/spib/select_noise](http://spib.rice.edu/spib/select_noise).
- [43] S. A. ALI, *Margin Based Learning for Robust Speech Recognition*, Ph.D. dissertation, N.E.D University, Dept. Computer Science and Information Technology., Karachi, Pakistan, 2015.

Comparative Study of Enhanced LIE, NPN, & DES Algorithm

Mrs. Mukta Sharma[#], Dr. R B Garg, Professor *

[#]Research Scholar, TMU, ^{*}Ex-Professor, University of Delhi

Abstract- The man has covered a long way from Stone Age to E-age (Electronic). Today, we live with technology. Technology has bridged the time and made our lives much easier. With the advent of technology, one can share their pictures, videos, money, emails etc. at a click of a button. Technology has so many advantages like one can navigate and check the routes, the nearest hotels, movie halls etc. ; can search for anything, can interact very easily with a person sitting 1000 of miles away, check the weather forecasts, transfer the money, shop online and so on. Everything comes with its pros and cons and so does the information technology. It has its own set of limitations like virus infection, hacking, spoofing, phishing, net extortion etc. One of the major fears is to transact online, there is a sense of insecurity of getting hacked and exploited. Researchers are working on ensuring the security while transacting online. One of the most significant topics of today is Cryptography. Cryptography is a technique to scramble the message into an unreadable message. Cryptography is a way of securing the message from unauthentic users. In case, an unknown person retrieves the message by hacking the system the person should not be able to read the real message.

This paper focuses on the need for cryptography, how cryptography can help saving the online transactions. A new symmetric key encryption algorithm named LIE (Let it Encrypt) has been designed using Java 1.6 (Eclipse, an IDE was used for its implementation). The paper commences with the basic introduction about security, security goals, mechanisms, cryptography, steganography etc. The paper is tactically divided into 4 sections. The first section comprises of the basic overview & structure of the algorithm. The second section depicts the implementation part, explains the code of the algorithm. Followed by its screenshots and in the end, a comparative analysis is illustrated depicting time and space for DES, NPN, and LIE algorithm.

Keywords— Cryptography, Symmetric & Asymmetric Cryptography, Plain Text, Cipher Text, DES, AES, NPN, LIE

I. INTRODUCTION

New inventions have always benefitted the society may it be the phones, computers, mobile phones etc. Computers have made lives easier and the internet has paced up the speed of doing things online. It has actually given a vision of staying connected and getting things done at a much faster pace in a much comfortable environment. In short, one can say the Internet has transformed everything from the way of doing

business, shopping, banking, studying, paying bills etc. and made it very easy and it also saves a huge amount of time. These benefits of the internet have attracted the society and most of the urban population are using the internet very often. The only reason to worry is the security; security from viruses, security from being trapped by hackers, pedophiles (in the case of kids), stalkers etc., fear of losing important data, and most importantly a threat of losing your hard earned money. The quality or state of being secure is to be free from danger. This paper would focus on ensuring the security while transacting online.

A. Classification of security goals

- Confidentiality- information should be confidential not in terms of storage of information but also while transmission of information. The information should be shown to only authentic users and if a hacker hacks the data; some unreadable format should be shown so that the original message is safe.
- Integrity-Information should be original, complete, uncorrupted. In short, information should not tamper.
- Availability-Information should be available whenever an authentic user needs it.

B. The above-discussed security goals fear the security attack.

- There is a threat to confidentiality via Snooping (unauthorized user can access/retrieve the file) and Traffic Analysis (Unauthorized user can monitor and later analyze the information and transaction done by someone else).
- Breaching security for integrity is possible through Modification (As the name suggest modification is done on the intercepted file by an unauthorized user), Masquerading (Spoofing or pretending to be some authorized user), Replay (hacks a message and try to replays it later on), and Repudiation (is done by either of the two authentic parties (sender/receiver) to deny information).

- Availability goal can be easily threatened by Denial of service attack (DOS will slow down or totally interrupt the services of a system).

C. Security Mechanisms

International Telecommunication Union-Telecommunication Standardization Sector (ITU-T, X.800) has recommended security mechanisms to provide better security [1].

- Enciphering- Technique to provide confidentiality by hiding or scrambling the data in an unreadable format. Can be attained by Steganography and Cryptography.
- Data Integrity- Data does not tamper can be achieved by hashing technique. Later results (check value) can be compared with the original message and if the size is same that means data is not tampered else it has some discrepancy.
- Digital Signature- Electronically signatures can be verified, digital signature uses the concept of asymmetric key encryption algorithm to attain confidentiality.
- Authentication Exchange-where two parties exchange some message to prove their identity to each other. Maybe by sharing and using the same key.
- Traffic Padding- To add some bogus or fake data to thwart the adversary's attempt to use the traffic analysis.
- Routing Control- Select and continuously change different available routes to avoid the rival from eavesdropping on a particular route.
- Notarization- the Third party may be involved to control the communication between two parties, very efficient way to restrict repudiation of data.
- Access Control- User needs to prove his authenticity by carrying unique passwords and Pin to access the data.

D. Techniques primarily used for protecting data

Steganography means Covered Writing was originated from Greek. It was extensively used during World War II. Now also it is being used for security and the messages are sent in a hidden manner. Unfortunately, these days' terrorists are also using steganography extensively they are attaching messages beneath images or audio files or video files and broadcast those images on any social network or chat rooms. For any user, it is just an image or an audio/video file but for another terrorist, it's a hidden message coveted in the file [3].

Cryptography is a Greek word which means Secret Writing. The security mechanisms listed above use cryptography primarily to resolve security. Cryptography is a technique used to transform messages to secret or unreadable messages.

E. Cryptography can be categorized into three types:-

- Symmetric Key or Secret Key- Sender and receiver share the key. The sender uses the key to encrypt the message and receiver use the key to deciphering the message.
- Asymmetric Key or Public Key- A set of two keys (public and Private) is used for the transaction. The Sender will send the message using receiver's public key which is globally announced and only the receiver can decipher the message with his private key.
- Hash Function- Uses mathematical transformation to irreversibly encrypt the message. This is applied to implement integrity & non-repudiation of data. Digital Signatures depicts the wide use of Hashing technique.

II. ALGORITHM

A. Overview

LIE is a block cipher, as shown below

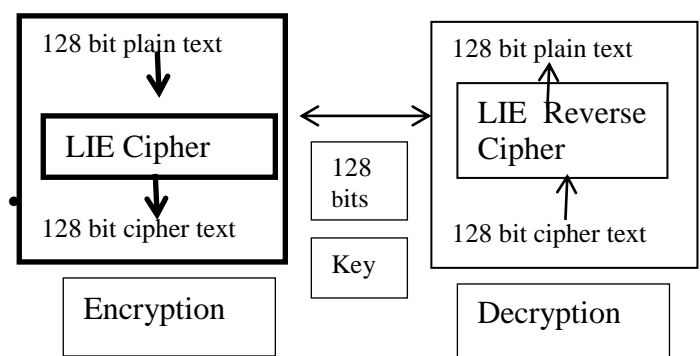


Figure 1: Basic structure of LIE

While encrypting in LIE, 128-bit Plain text is given as an input and a 128-bit cipher text is retrieved as an output. Similarly, while decrypting 128-bit cipher text is converted into 128-bit plain text. A 256 bit Key is used for both encryption & decryption process.

B. LIE Structure-

- **Block Size-** The block size is 128 bits. The encryption process begins by permutations of the 128-bit plaintext using the initial permutation.
- **Feistel Network-** LIE is based on Feistel network like DES, Blowfish etc. LIE will divide the message into 64 bits.
- **Key Size-** Key size should be 128 or more for better security. Therefore, the key used in LIE is 256 bits for ensuring security.
- **Key Generation-** [2] the first phase involves generation of 256-bit key. Earlier the Key was generated using the timestamp. The key matrix was initialized with all zero values. The timestamp was captured. All the digits were added to find a single digit number. That location in the key array was marked as '1'. The location

number digit on left & right were further added to get the next location and henceforth. Once all values are found 1's complement was done on key. The flaw was identified late in this method of generating the key. One being the attributes of timestamp can be identified very easily. It offers very less number of combinations. Also, the single digit found at first step gives only 9 combinations for any hacker to try and generate the key.

Identifying these issues, the approach to generate key was changed. Now it is based on a random number generated by rolling of dice. This number will be called 256 times to generate a number for each location for the key. As known, this will generate number only from 1 to 6. Thus, the output of this function will be checked for being an even number or odd number. If a number is even then '0' will be placed at the location 'I' of key matrix else '1' will be entered. This gives equal probability to both '0' and '1' to be assigned to any location in the key array and also offers a well-known randomness of rolling of dice.

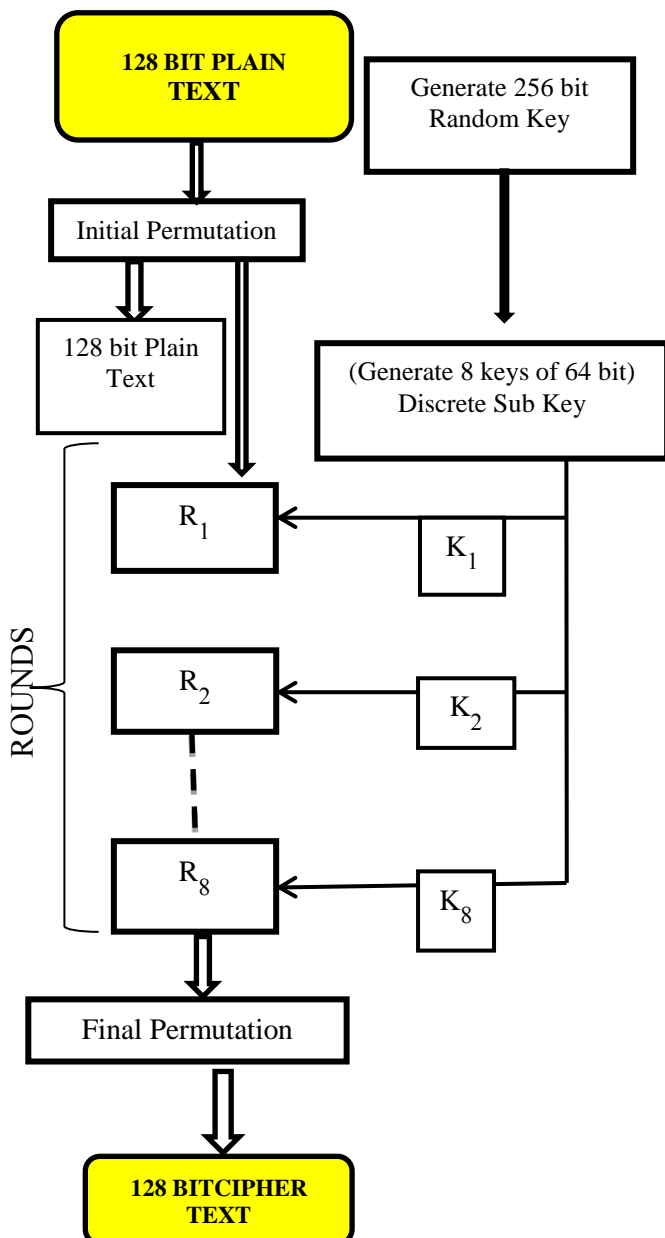


Figure 2: Process of Encryption

- *Initial and Final Permutation*

The initial and final permutation arrays are designed to bring in the confusion at the first step and the final step of the algorithm. These are designed keeping in mind the confusion-diffusion principles given by Claude Shannon. The first to make it difficult to identify the relation between cipher & the key & the second is to spread the plain text across the wide cipher text.

- *Rounds*

The algorithm has 8 rounds in total. For each round, a separate key is involved. In cryptography, there is an identified rule that if for each round a complete discrete key is available then even 4 rounds give a more secure cipher as compared to any higher number of rounds. Here, 4 uniquely discrete sets of key are available. Even then to maintain security 8 rounds are used.

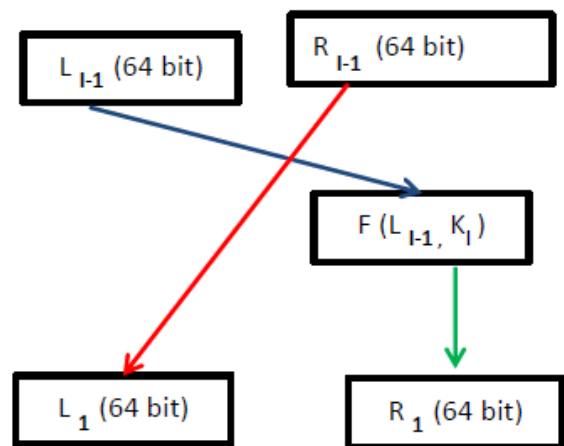


Figure 3: Round in LIE

- *Function*

The function is the core part of the algorithm. The function here has 3 main steps. The first step involves another inner permutation of the text. This takes it to next step where a circular left shift is done. Lastly, the XOR operation is performed on the text along with the key being used for that specific round [2].

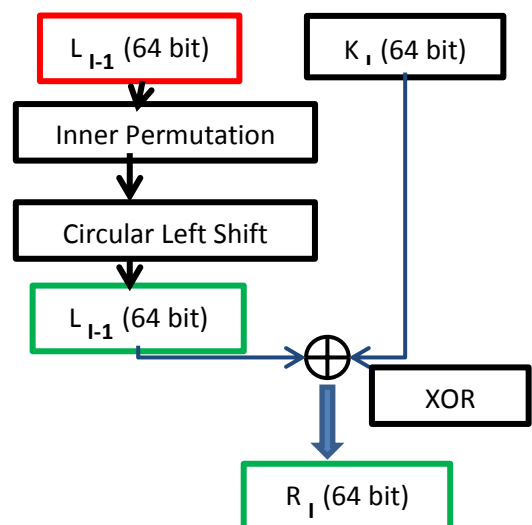


Figure 4: Function (F)

III. PSEUDOCODE

- Step 1. Initialize Key matrix $k[] = 0$
- Step 2. For $I \rightarrow 0 \rightarrow 255$
Generate Random number using rolling of dice & save in variable dice.
- Step 3.
If $\text{dice} \% 2 == 0$ then $\text{key}[i] = 0$
Else $\text{key}[i] = 1$
- Step 5. Generate subkeys k_1 to k_8 using subkeys matrices.
- Step 6. Take 128-bit plaintext as input \rightarrow PT
- Step 7. Perform Initial Permutation.[2]
- Step 8 While $I < 64$
Step 9 Divide PT(128 bits) into L_0 & R_0 each 64 bit.
- Step 10. $L_i = R_{i-1}$
 $R_i = F(L_{i-1}, k_i)$
- Step 11. $F(L_{i-1}, k_i)$
a) Permutate L_{i-1} using Inner Permutation
b) Perform Left Circular Shift
c) L_{i-1} XOR K_i
- Step 12. $I \rightarrow i+1$
- Step 13. Obtain $CT' = R_{64}L_{64}$
- Step 14. $CT =$ Perform Final Permutation.

LIE's decryption process works in reverse order of encryption process. Therefore, the logic of decryption is very simple. To attain plain text from cipher text, just backtrack the encryption process which means starting from final permutation (which is the final step for converting plain text to cipher text) and tracking it back from subkey K_8 to K_1 [4].

IV. IMPLEMENTATION AND SCREEN SHORTS OF LIE

```
temp= rounds(plaintext16,innerPerm,keys);
//Code for Final Permutation
for(int i=0; i<128; i++)
{
    // System.out.println(finalPerm[i] + " " + plaintext16[i]);
    finalciphertxt128[i]= temp[finalPerm[i]];
}

System.out.println( "\n "+"before final permutation");
for(int i=0; i<128; i++)
{
    System.out.print(temp[i]+ ",");
}

System.out.println( "\n ");
System.out.print("final cipher"+ "\n");
for(int i=0; i<128; i++)
{
    System.out.print(finalciphertxt128[i]+ ",");
}
long endTime = System.nanoTime();
System.out.println(" \n Took "+(endTime - startTime) + " ns");
```

Figure 5: Encryption Code Snippet

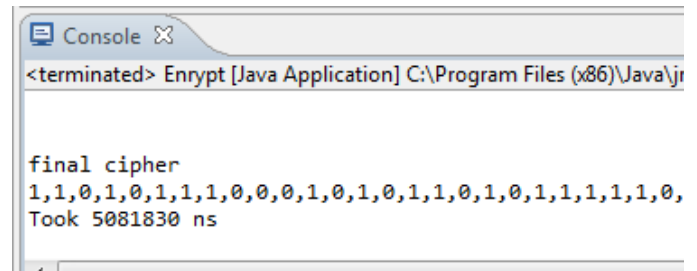


Figure 6: A section picked up from Obtained output.

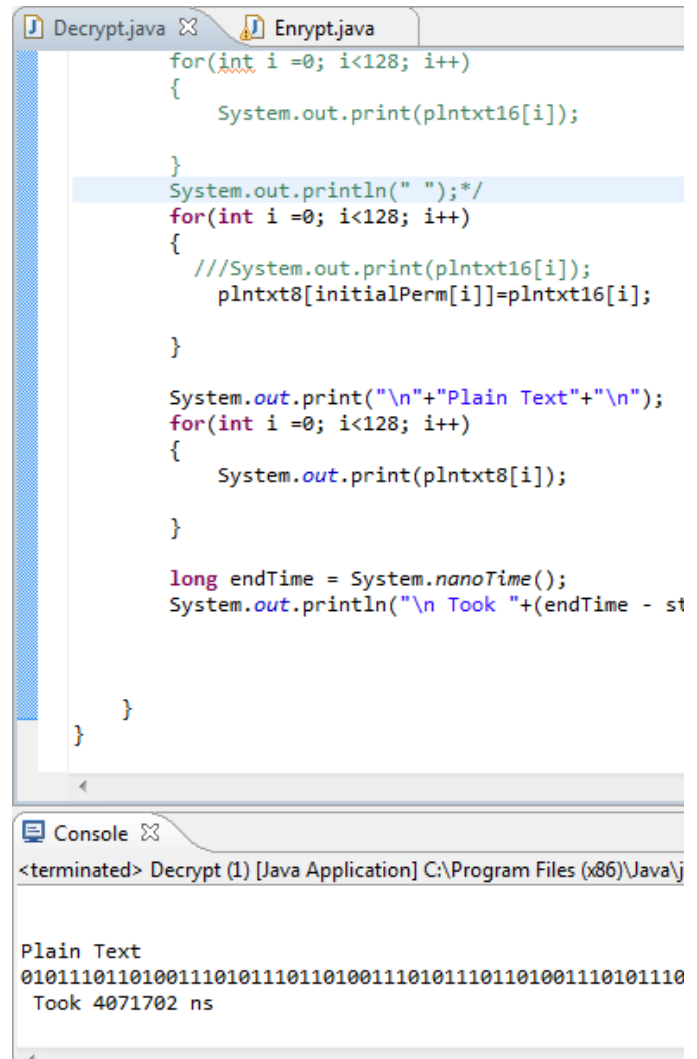


Figure 7: Decryption Code Snippet and part of Output obtained.

V. COMPARISON OF LIE, NPN, AND DES

LIE, NPN, and DES are symmetric key encryption algorithm. LIE & DES are based on Feistel network. NPN is not based on the concept of Feistel network. DES was conceptualized in 1975 and was registered in 1979. NPN was introduced in 2014 and LIE came into existence in 2016. DES and LIE use the concept of Confusion and Diffusion. NPN is based on Prime numbers and Pseudo-random numbers

The complexity of algorithms is checked on two main factors time & space. The memory usage for these algorithms

is mentioned below. The building blocks parameters of these algorithms like key size block size & number of iterations or rounds decide the memory required by the algorithm. Here, LIE has a key size of 256 bits to enhance the security as compared to DES which has 56-bit key. The block size of LIE is 128 bits, DES is 64 bits and number of iterations in LIE is 8 rounds and DES it is 16 rounds.[5] Classes and 2d Arrays were used while implementing the code in java. LIE, uses 1 2dimension array and 1 class, and DES uses 14 2 dimension Arrays and 9 classes.

Time Comparison is depicted with the help of Table 1 and figure 8 and 9 for both encryption and decryption.

	NPN	DES	LIE
Encryption Time (nano sec)	429696933	319453496	5081830
Decryption Time (nano sec)	411487764	153947	4071702

Table 1: Encryption/ Decryption time taken

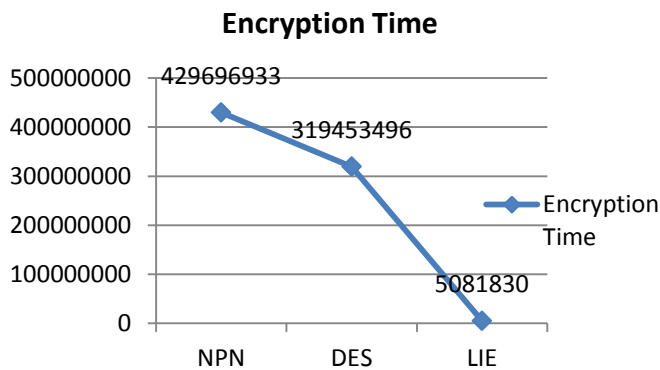


Figure 8: Screen shot of Encryption Process using LIE Algorithm

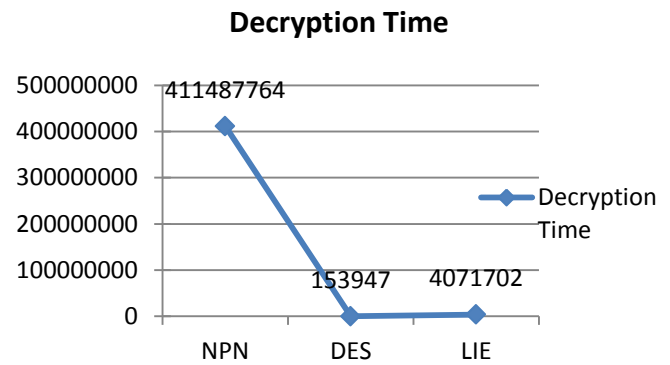


Figure 9: Screen shot of Decryption Process using LIE Algorithm

VI. CONCLUSION

LIE seems to be less time and space consuming, based on the analysis mentioned above. LIE has been tested theoretically on various grounds of Cryptography like KEY size, block size, Number of rounds etc. for enhancing and ensuring security.

VII. FUTUTRE SCOPE

Algorithm has been designed and checked only for basic grounds like time and space. Next research will focus on testing parameters based on security. Algorithm needs to be compared with some more algorithm like AES, blowfish etc.

VIII. REFERENCES

- [1] Forouzan, B.A., & Mukhopadhyay, D., "Cryptography and Network Security", McGrawHill, ISBN-13: 978-0-07-070208-0, 2nd Ed.
- [2] Sharma, M., Dwivedi, S., & Garg, R.B., "Let It Encrypt", International Journal of Computer Applications, 973-93-80889-75-8, Volume 128, No. 8, pp. 9 to 15.
- [3] Sharma, M. & Garg, R.B., "Steganography is the art of Hiding Data", IJARSE, 2319-8354(E), Vol. 4, No. 1, pp. 1801 to 1809
- [4] Sharma, M. & Garg, R.B., "Random Key & the Nth Prime Number based Symmetric key Encryption Algorithm", IJATES, 2348-7550, Vol. 2, No. 1, pp. 309-317.
- [5] Sharma, M., Dwivedi, S., & Garg, R.B., "Comparative Analysis of NPN Algorithm & DES Algorithm", ICRITO, Amity 2014, IEEEExplore, 978-1-4799-6896-1/14/\$31.00,

LEGACY PROGRAM ESTIMATION

Harmeet Kaur
Ph.D. (Computer Applications)
Research Scholar, Punjab Tech.
University Jalandhar, India.

Shahanawaj Ahamad
Asth. Professor, College of Computer
Science & Engineering
University of Ha'il, K.S.A.

Govinder N. Verma,
Professor & Principal, Sri Sukhmani
Institute of Engg. & Technology, Dera
Bassi, Punjab, India.

Abstract—Software metrics support various complexity estimation techniques. This paper shows that how a set of software metrics can be used to evaluate the complexity of the legacy system. The paper presents the development of a framework and its applications. The metrics can be used in the measuring the complexity the software. To measure the decrement in complexity is one of the goals of the estimation process. As the legacy software systems are an important asset of the organization so they cannot be ignored or discarded. The collection of metrics has been used to estimate the complexity of the legacy software system to make decision on the reengineering of the legacy software. This paper demonstrates a metric framework which has been used for complexity estimation. The framework consists of various phases with applications on various open source programs written in C, C++ and COBOL

Keywords- Program; Legacy; SDLC; CW; LOC.

I. INTRODUCTION

In few last decades, software complexity has created a new era in computer science [1]. Software complexity could be defined as the principle driver of cost, reliability and performance of software. In any case, there is no common agreement on software complexity definition, yet the greater part of them is dependent upon use perspective of software complexity [2], "software complexity is the level of challenge in analyzing, maintaining, testing, designing and modifying software ". In other words, software complexity is an issue that is in the whole software development process and each phase of software development life cycle (SDLC). Software complexity is a broad term and has attracted various workers, and many metrics have been proposed to measure the complexity of the software since 1976 [5]. This estimation is particularly basic in the software management and has important role in project accomplishment. Complexity strongly impacts the needed effort to analyze and portray requirements, design, code, test and debugging the system during the development phases of software. In maintenance phases, complexity indicates the trouble in error correction and the needed effort to change distinctive software module.

The expanding vitality of software measurement and metrics accelerated the growth of new software complexity measurement and in software engineering metrics are essential for estimations for project planning and project measurement. The increased demand for software quality has

brought about higher quality software and these days quality is the fundamental differentiator between the software products. Due to this reason software designers and developers require substantial measures for the assessment, improvement and acceptance of software product from the initial stages. Nowadays software measurement assumes an essential part for measuring complexity and quality of software. Since software complexity influences software development effort, cost, testability, maintainability and so on. Thus it is indispensable to measure the software complexity in every software development phase. A variety of metrics have been proposed for measuring software complexity.

II. LITERATURE REVIEW

The predominant question is "What is Complexity?" IEEE outlines software complexity as the degree to which a system or component has a design or execution that is challenging to comprehend and verify [4]. Through the years, research on measuring the software complexity has been carried out to comprehend, what makes computer programs difficult to understand. Few measures have indicated concern to propose the complexity measures whose calculation itself is not complex. A major force behind these efforts is to increment our capability to predict the effort, quality, coding efficiency, cost or all of these. Major complexity measures of software that refers to effort, time and memory expended have been utilized in the form of Halstead's software metric [3], McCabe's cyclomatic complexity [6], complexity Metric by Klemola's KLCID [17], Wang's cognitive functional complexity [19] and many others.

The degree to which characteristics that hinder software maintenance are available is called software maintainability and is determined principally by software complexity, the measure of how demanding the program is to comprehend and work with. It has been evaluated that about 40 to 70% of the yearly software expenditure is spent on maintenance of software so if the complexity of the software is comprehended by the programmer than the maintenance procedure could be balanced. Maintenance characteristics that are influenced by complexity incorporate software understandability, software modifiability, and software testability. Different methodologies may be taken in measuring complexity characteristics, for example Baird and

Noma's approach, in which scales of estimation are divided into four types.

In light of the fact that a great part of the software complexity measurement has been done in the last few years, numerous diverse techniques are being utilized. [5] has recommended that program size, data structures, dataflow, and flow of control can influence maintenance. Various measures have been developed to assess each of these aspects, and numerous hybrid measures have been created to acknowledge more than one concurrently. One of the central issues in software engineering is the inherent complexity. Since software is the consequence of human innovative activity, cognitive informatics assumes important role in comprehending its basic attributes. [19] displays one of the principal aspects of software complexity, by inspecting the cognitive weights of basic software control structures. Taking into account this methodology another idea of cognitive functional size of software is developed. The cognitive functional size furnishes an establishment for cross-stage examination of analysis of complexity, size, and comprehension effort in the design, execution, and maintenance phases of software engineering. Few of the methods and techniques are discussed here and plethora of literature is available on various methods and techniques used for software complexity measurement.

For the last few decades greater importance is given for measuring the software characteristics [2]. It is just by such a procedure of estimation that it will be conceivable to determine if new programming techniques are having the impact in lessening the issues of reliable software production. Although number of the characteristics of interest, for example, clarity, simplicity of testing and maintenance, and so forth., are exceptionally subjective thus analyses have been performed to related subjective reviewing of programs with measured structural characteristics of source programs [1]. Cost estimation strategies are focused around past experience and a complexity measure of software gives a premise for an objective investigation of past programming knowledge. The issue then is what constitutes complexity measure. The parts of a system which make it easy to a developer, a manager, or a maintainer are very distinctive. Also program straightforwardness is not measurable in terms of variable or two. As far as software metrics are concerned much taxonomy has been used to describe the metrics. Since the pioneering work of Halsted numbers of software metrics have been developed. On the basis of functionality complexity metrics can be divided into two:

- a) Static Complexity: This metric explores the textual information in the source code of the program.
- b) Dynamic Complexity: It deals in exploring the semantic effects of the code in operation at run time.

With the intent of providing some structure and organization to the ever increasing number of complexity metrics several taxonomies have been put forward for example [9], have categorized the metrics into static, control organization, volume, history and data organization metrics.

III. ASPECTS

Complexity in Data: The complexity in the legacy system is due to data also.

Complexity in Implementation:

As legacy software systems are difficult to implement thus implementation of such systems also contributes in complexity.

Complexity in Documentation:

It is another factor which increases the complexity. It is not easy to document the legacy software systems and thus enhances complexity.

Complexity in Time:

Since the legacy programs are slow but they are used by the organizations to meet their goal but the time has an important role to play as far as the legacy program is concerned. As the time increases the complexity also increases which affects the expectations of the organization or user.

Complexity in Internal sources:

As Internal sources include modern hardware, e.g. super-scalar processors ever changing technology poses threat to the existing systems and the existing systems are not able to compete with the new technology. Sometimes software consists of two or more than two software's e.g. banking software consists of two software which are dependent on each other i.e. internet and telecommunication system if either of the two fails it is difficult for the banking system to run.

Complexity in External sources:

These sources include the requirements for evolving already successful systems. The advancement in the technology increases the expectations of the users thus the external sources also increases the complexity of the existing systems which are important for the organization. It arises how the systems are used and the environment in which these are used.

Complexity in Maintenance:

The maintenance includes great part of the assets of the organization in terms of staff, funds etc. A few sources estimate that activities during the maintenance phase may consume as much as 75 to 90 percent of total product lifetime costs. It contributes in increasing the complexity of the system.

Complexity in Size:

The size of the legacy software is also responsible for enhancing the complexity of the software. If the program is too large it is difficult to understand the program and it requires time to build or make corrections.

Complexity in control flows:

The presence of loops, functions, conditions also increases the complexity irrespective of the fact whether the program is small or large in size.

Complexity in Use:

As legacy software are based on outdated technology they are not easy to use and their use poses complexity while interacting with the system.

IV. LEGACY

Although the emergence of new technologies and techniques in the area of information technology has changed the working environment but Legacy software still is valuable resources for the organizations. One of the primary perspectives that compel organizations to keep up its legacy system in business is the exceptionally valuable functionality provided by the system, which can't be effectively executed in numerous brand-new enterprise solutions. Then again, the

resistance to put new set up may adversely influence the development of the organization as far as its compatibility with the recent business needs is concerned (e.g. ecommerce models). The issue is, is it essential to supplant most of the current software systems. There will be different thoughts on this issue some will concur, and some will contradict this thought. If the changes are to be made in the database and customer interface it is useful to change or replace the present system so it can meet the client requirements and contend with the evolving technology. The choice whether to keep the present system or to supplant it depends on the complexity, quality and effort of the present system furthermore on the requirements of the customer. On the other hand if the changes to be done in the software are too small then it might be possible to make those changes instead of supplanting it or vice-versa.

V. FRAMEWORK

The frame work of the study consists of various phases:

V.I Defining the Problem:

In this phase the problem is defined and objectives of the estimation that need to be estimated.

V.II identifying the metrics:

A metric framework has been proposed for complexity estimation of legacy program. Various types of metrics have been proposed for measuring the complexity of the software. These metrics have been categorized into various groups depending on the aspect they measure. For the present study we have taken various complexity metrics which are as:

Table 1. Study of complexity matrices

S.No.	METRICS	USE
1	Lines Of Code (LOC)	Use to measure the size of code by counting its lines.
2	Mccabe Complexity	Use to measure cyclomatic complexity
3	Halstead method	Use to measure the difficulty, volume and effort.
4	Cognitive weight Method	Use to know degree of difficulty.

V.II identifying the programs:

The programs are taken from open source to estimate the complexity. Basically we have chosen programs written in COBOL, C and C++.

V.IV Estimation:

The complexity of the programs taken from the open source is measured using various methods as stated in first phase of the framework. The methods selected are applied on these programs and their complexity is measured. The formulas specified in complexity estimation methods are to be used to produce estimate values for the characteristics to be measured.

V.V Exploring the Results:

After the estimation the results are noted and compared.

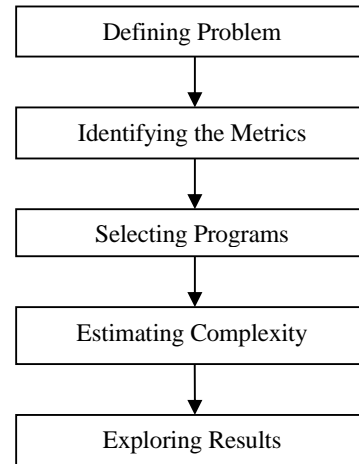
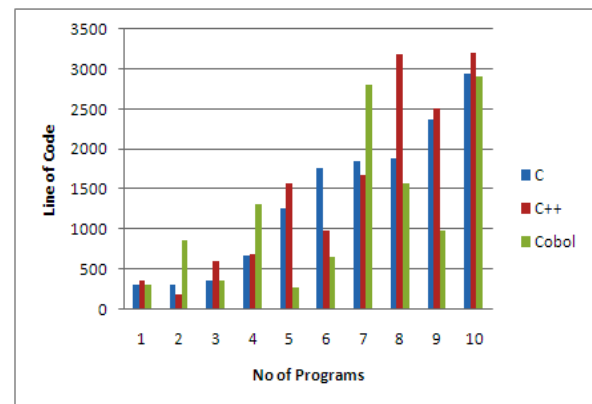


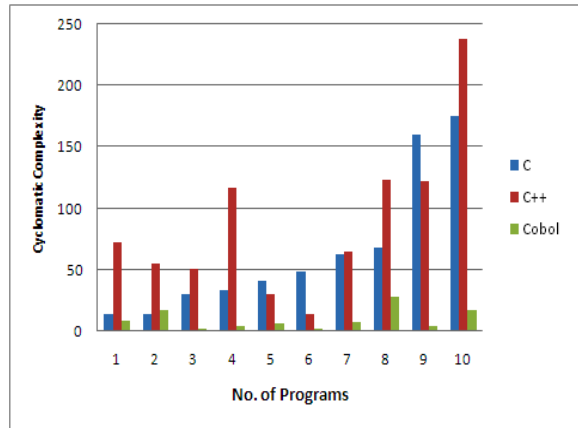
Fig.:1 Framework for estimating the complexity

VI. RESULTS

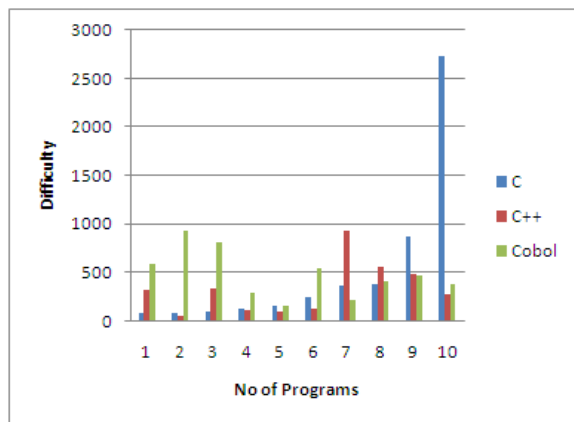
Complexity estimation of the legacy program was done using various metrics as stated earlier in the paper. For carrying the research work the programs written in COBOL, C and C++ were selected from open source and during the estimation it was observed that programs written in COBOL are complex and have not shown regular trend in Loc and Cc and no effect in case of CW and difficulty was observed whereas inverse relationship in case of difficulty and Cc was observed in COBOL. In contrast to this it was observed that in C, there is direct relation in Loc, Cc (Cyclomatic complexity) and difficulty as well as in CW whereas no direct relation observed in Loc, Cc, difficulty and CW was seen in case programs written in C++ it might be due to classes, objects etc in the programs. The complexity in the COBOL was more due to structures and size whereas programs written in C++ are less complex as compare to the programs written in C. It is observed the programs with more control structures, logical decisions and control paths are more complex than those where the number of such structures is less. As far as the size of the program is concerned it is also responsible for enhancing the complexity of the program as larger programs are difficult to handle.



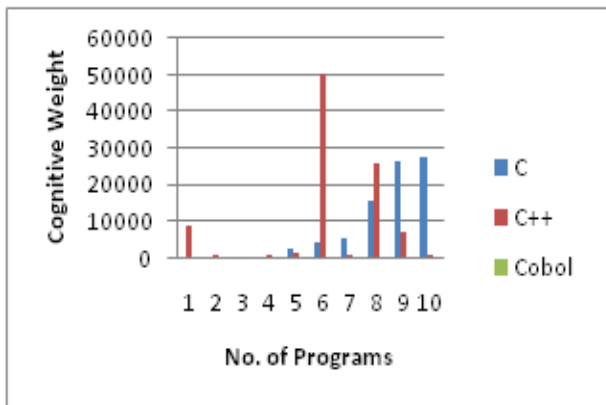
Graph1: Showing the Loc of Programs



Graph2: Showing the Cyclomatic Complexity of Programs



Graph3: Showing the difficulty of Programs



Graph4: Showing the cognitive weight of Programs

VII. PRESENT ISSUES IN SOFTWARE COMPLEXITY MEASUREMENT

Various types of complexity like structural complexity, functional complexity, psychological complexity etc. have been discussed by the researchers. It was also observed that functional complexity focuses on the complexity that results from factors related to system structure and connectivity, whereas, control flow complexity has been discussed in terms of weyuker's properties. One of the studies aimed at

finding the relation between complexity and security *i.e.* it was explored whether more complex code is less secure or vice versa. Many of the studies have explored various well known complexity estimation methods like McCabe's cyclomatic complexity, Halstead method, Loc *etc.* but a few of them have given the new ways to measure these metrics. The new methods for estimating complexity of business process and aspect oriented metrics has also been discussed in the literature. A graph-theoretical complexity metric to measure object-oriented software complexity has also been described and these studies have shown that their exist a close relation between inheritance and the object-oriented software complexity and has revealed that misuse of repeated (multiple) inheritance will increase software complexity and prone to implicit software errors.

System complexity comprised of internal and external complexity it was examined that system complexity ordinarily influences characteristics for software reliability, maintainability, and testability of software systems which are recognized as of utter significance in composing an improved software product. For accomplishing these software qualities, system complexity must be regulated by modularizing the system into different modules of suitable complexities. Software complexity measures are regularly proposed as suitable indicators of diverse software quality traits.

An incredible deal of effort is currently being dedicated to the study, analyses, expectation, and minimization of expected software maintenance cost, much sooner than software is conveyed to users or stakeholders. It had been evaluated that, on an average, the effort spent on software maintenance is as expensive as the effort used on all other software stages. Ways to mitigate software maintenance complexity and increased cost may originate in software design.

In the past data complexity has been overlooked in measuring the software complexity however now few of the studies have done on data complexity and data scope complexity. In the meantime work to quantify object oriented and procedure oriented programming has been done. Many researchers have concentrated their work on measuring the cognitive weight unpredictability and the information flow complexity which is dependent upon the information held by the program. Much of work has been done on measuring the software complexity yet this field needs further research for the advancement of software complexity measurement techniques and strategies.

VIII. CONCLUSION

Before estimation, a clear specification of what is being measured and why it is to be measured must be formulated. This description should be supported by a theory of programming behavior. As Software estimation is the basis to change software development in to engineering practice so it must be taken seriously. Estimation should be based on scientific principle and must be able to meet the objectives that are the estimation should be goal oriented. The complexity measurement is in existence for the last decade or two but still it lacks in some standardized way which is applicable to all the software evaluating complexity. The objective here is, however, not to argue for various complexity estimation methods which are available but the

goal is to assess the complexity of the legacy programs written in COBOL, C and C++. It has been emphasized that complexity estimation of the software or the program must be done through the life cycle of the software. To be precise software measurement particularly complexity estimation is an important activity, and must be carried out meticulously so that keeping in view the results the reengineering of the legacy programs can be undertaken. We are working on estimation of complexity applying more methods and programs to enhance the accuracy.

- [20] Zuse, H, "Criteria for Program Comprehension Derived from Software Complexity Metrics," Proceedings of the Second International Workshop on Software Comprehension, IEEE, Capri/Italy1993: pp.8-16.

REFERENCES

- [1] IEEE Computer Society: IEEE Standard Glossary of Software Engineering Terminology, IEEE Standard 610.12,1990.
- [2] J. C. Munson and T. M. Khoshgoftaar, "The detection of fault-prone programs," IEEE Transactions on Software Engineering, Vol. 18, No. 5, 1992, pp. 423-433.
- [3] G. K. Gill and C. F. Kemerer, "Cyclomatic complexity density and software maintenance productivity," IEEE Transactions on Software Engineering, Vol. 17, No.12, 1991, pp.1284-1288.
- [4] Halstead, M.H, "Elements of Software Science," Elsevier North, New York, 1977.
- [5] McCabe, T.H, "A Complexity Measure", IEEE Transaction on Software Engineering, SE - 2, 6, 1976, pp. 308 - 320.
- [6] Misra, S and Misra, A.K., "Evaluating Cognitive Complexity measure with Weyuker Properties," Proceeding of the 3rd IEEE International Conference on Cognitive Informatics, 2004.
- [7] E. Brito, F. Abreu, and W. Melo, "Evaluating the impact of Object-Oriented Design on Software Quality," Proceedings of 3rd International Metric Symposium, 1996, pp.90-99.
- [8] M. Marchesi, "OOA metrics for the United Modeling Languages," Proceedings of 2nd Euromicro Conference on Software Maintenance and Reengineering, Palazzo degli Affari, Italy, 1998, pp. 67-73.
- [9] M. Genero, M.E. Manso, M. Piattini, et al, "Early metrics for object oriented information systems," Proceedings of 6th International Conference on Object Oriented Information Systems, London, UK, 2000, pp.414-425.
- [10] M. R. Woodward, M. A. Hennell and D. A. Hedley, "A measure of control flow complexity in program text," IEEE Transactions on Software Engineering, Vol. 5, No. 1, 1979 pp. 45-50.
- [11] R. D. Banker, M. D. Srikant, C. F. Kemerer, and D. Zweig, "Software complexity and maintenance cost," Communications of the ACM, Vol. 36, No. 11, 1993, pp. 81-94.
- [12] R. Subramanyam and M. S. Krishnan, "Empirical analysis of CK metrics for object-oriented design complexity: Implications for software defects," IEEE Transactions on Software Engineering, Vol. 29, No. 4, 2003, pp. 297-310.
- [13] S. Chidamber, and C. Kemerer, "A Metrics Suite for Object Oriented Design," IEEE Transactions on Software Engineering, 20(6), 1994, pp. 476-493.
- [14] Sheng, Yu, and Shijie, Zh., "A survey on metric of software complexity," 2nd IEEE International Conference on Information Management and Engineering, 2010, pp.352-356.
- [15] Tian, J., and Zelkowitz, M. V, "Complexity Measure Evaluation and Selection," IEEE Transactions on Software Engineering, vol. 21, No. 8: 1995, pp. 641-650.
- [16] T. Menzies, J. Greenwald and A. Frank, "Data mining static code attributes to learn defect predictors," IEEE Transactions on Software Engineering, Vol. 33, No. 1, 2007, pp. 2-13.
- [17] Tuomas Klemola and Juergen Rilling, "A Cognitive Complexity Metric Based on Category Learning," IEEE International Conference on Cognitive Informatics, 2003.
- [18] V. Basili and A. Turner, "Iterative Enhancement: A Practical Technique for Software Development," IEEE Trans. Software Eng., Vol. SE-1, 1975, pp. 390-396.
- [19] Wang, Y., and Shao, J, "Measurement of the Cognitive Functional Complexity of Software," IEEE International Conference on Cognitive Informatics, 2003.

GSM Based Bank Vault Security System

Ripan Kumar Ray

Department of Electronics and
Telecommunication Engineering
University of Development
Alternative (UODA)
Dhaka, Bangladesh

Muhammad Afsar Uddin

Department of Computer Science &
Engineering
University of Development
Alternative (UODA)
Dhaka, Bangladesh

Syed Foyzol Islam

Department of Electronics and
Telecommunication Engineering
University of Development
Alternative (UODA)
Dhaka, Bangladesh

Abstract—Automated security system is a useful addition, where safety is an important issue. By this project a security system has been designed to protect the bank vault from thief or unauthorized person. This security system consists of four sensors, IP camera and GSM (Global System for Mobile communication) module. Sensors are Sound sensor, Motion sensor, Laser sensor and Gas sensor. GSM modem is used to send warning SMS to dedicated phone number. IP camera is utilized to monitor vault room remotely. When any of four sensors detect something wrong, then a warning SMS is automatically transmitted to a dedicated phone number and also a warning alarm turn on through Arduino microcontroller and GSM module. As a security system of bank vault has been designed and it has been tested several times and found most suitable security system.

Keywords— Arduino UNO microcontroller, GSM module, IP camera, Security system, Sensor, SMS.

I. INTRODUCTION

Security is the degree of protection from harm. It applies to any valuable asset, such as a person, dwelling, community, nation, or organization. In today's age of digital technology and intelligent systems, automation, security system has become one of the fastest developing application-based technologies in the world.

A bank vault is a secure space where money, valuables, records and documents can be stored. It is intended to protect their contents from theft, unauthorized use, fire, natural disasters, and other threats, just like a safe.

All the branches are under the surveillance of CCTV cameras, alarm systems, emergency buttons, etc. The CCTV cameras need to be monitored continuously in the control room by a human being which is very difficult work; especially at nights. The alarm, emergency button also needs to be pressed manually. This conventional system requires a lot of manpower.

By observing the Bank vault security system that banks has security systems that suffer the following drawbacks:

- Never used Laser technology
- Can't be activated automatically
- Can't respond immediately
- Most of CCTV cameras are ordinary not IP enabled

In this paper, an integrated four-level security system of Bank vault, consisting of IP camera & GSM module has been proposed which fulfills all these requirements. All systems work independently, but are incorporated into a single automated system for practical implementation. In the next section, the integrated architecture of the system is further elaborated. Finally, the conclusion and future directions of proposed "GSM Based Bank Vault Security System" is also given.

II. PROPOSED SECURITY SYSTEM

To Stop the Bank vault robbery, a GSM based security system named- "GSM Based Bank Vault Security System" has been proposed. By this project more security level of Bank vault has been ensured.

There have been done more research and work in GSM Based automated security system. Several security systems were developed in [1], [2]. In [1], microcontroller ATmega16 are connected together and also connected with an alarm system and GSM modem. In [2], developed a multilayer Bank security system using microcontroller ATmega16 which is integrated RFID, PIR sensor, IRIS and Fingerprint scanner and alarm system.

In this proposed GSM Bank vault security system, four sensors have been used. Also an IP camera and GSM Module have been used.

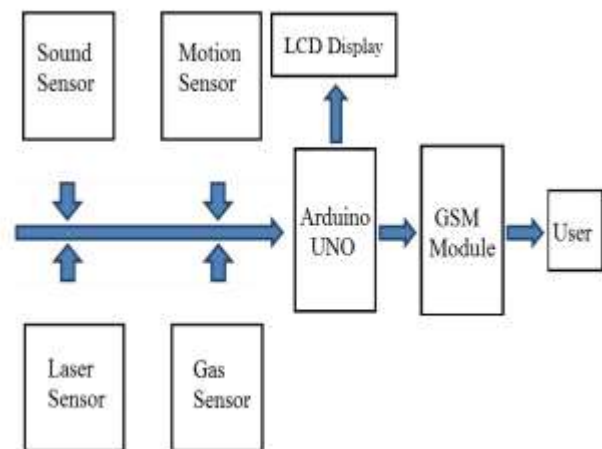


Figure 1. Simplified Block Diagram of the proposed security system

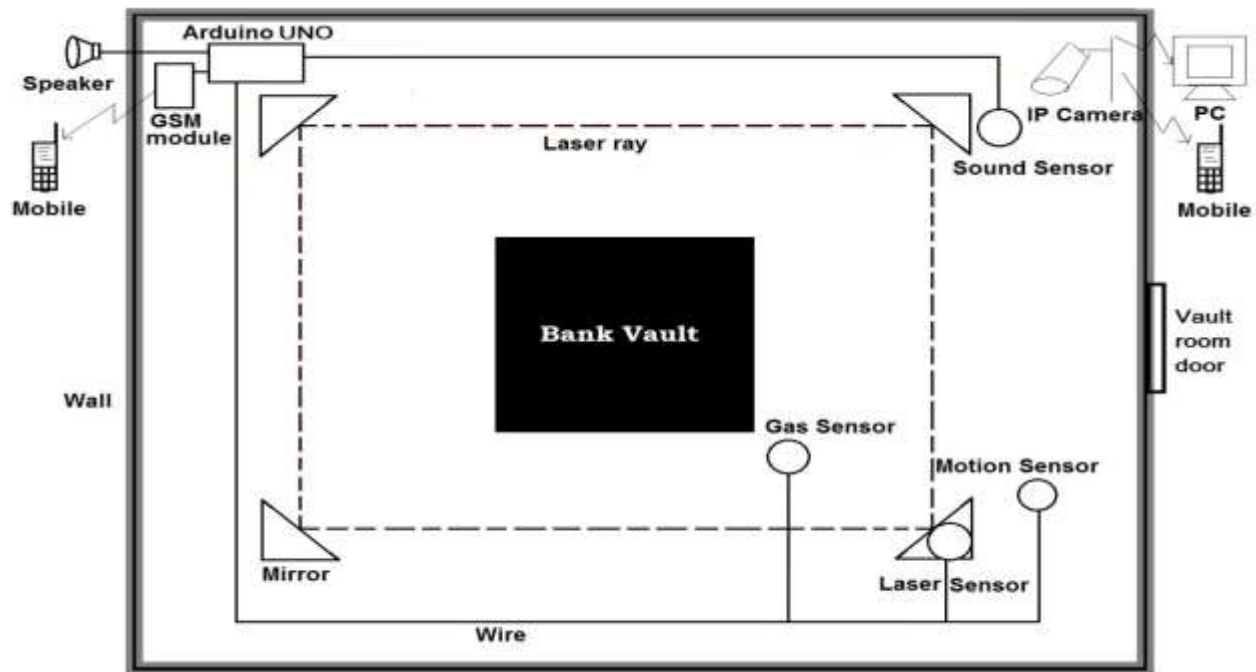


Figure 2. The Basic Architecture of GSM Based Bank Vault Security System

Figure 1 shows the simplified block diagram of the proposed security system. The figure shows that the system design comprises various hardware modules. The primary modules are sensors (sound, motion, laser and gas) which send signals to the Arduino when any of sensors activated in the vault room. All sensors are connected to the Arduino UNO Board and Arduino also connected to the alarm system to create an alarm and GSM modem to send a warning message.

III. SYSTEM COMPONENTS

Figure 2 shows the basic architecture of GSM Based Bank Vault Security System. In this section major components describe briefly.

A. Arduino UNO

The Arduino UNO is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal. Its input voltage is 6-20V, flash memory 32 KB [3]. This module is very important in this system. All sensors and GSM module connect to this module. When any sensor sends wrong signal to the Arduino board, then it creates an alarm and send a warning message to phone through GSM modem.

B. GSM Module

SIM900 board has been used, which supported Quad-Band 850 / 900/ 1800 / 1900 MHz. It's directly connected with the Arduino UNO board shown in figure 2. It consists of SIM Card holder, GSM Antenna, RS232 serial port [4]. This is Low power consumption device. This module helps us to send messages to the dedicated phone number.

C. Sensors

A sensor is an object whose purpose is to detect events or changes in its environment, and then provide a corresponding output. Four sensors have been used in this proposed system. These are- Sound sensor, Motion sensor, Laser sensor and Gas sensor.

1) *Sound sensor*- A device, transducer, or object which senses sound. It works by mimicking the human body process that involves the ears and signal transmission to the brain. Microphones are sound sensors that convert a sound signal into a voltage or current proportional to the detected signal [8]. When any kind of sound produces inside the vault room, then the sensor will be activated and also an alarm and SMS will be sent to the dedicated phone.

2) *Motion sensor*- Passive Infrared sensor (PIR sensor) acts as a motion sensor. All objects with a temperature above absolute zero emit heat energy in the form of radiation. Usually this radiation is invisible to the human eye because it radiates at infrared wavelengths. PIR has been working entirely by detecting the energy given off by other objects. PIR sensors don't detect or measure "heat"; instead they detect the infrared radiation emitted or reflected from an object [7]. So when an unauthorized person tries to enter the vault room, then PIR sensor detects it and send a signal to the Arduino, then Arduino creates alarm and send warning SMS through GSM.

3) *Laser sensor*- LDR has been used as a laser sensor. LDR is low cost and easily available. Laser ray directly reflects to the LDR via several mirrors [5]. Laser light is invisible as a result, when someone tries to come closer to the vault, then the

laser light interrupts and a warning message will be sent to the dedicated phone and also create an alarm.

4) *Gas sensor*- In this proposed system, MQ5 gas sensor has been used. This module is useful for gas leakage detection. It is suitable for detecting H₂, LPG, CH₄, CO, Alcohol [6]. When someone leaks this types of gas in the vault room, then the sensor detects gas and suddenly alert us by creating alarm and sending a message to the phone.

D. IP camera

An IP camera or Internet protocol camera is a type of digital video camera commonly used for surveillance. It can send and receive data via a computer network and the Internet [9]. Live video can be viewed from any computer, anywhere, and also from Smartphone's and other devices. So vault room can be monitored from anytime and anywhere.

IV. SYSTEM OPERATION

Figure 3 shows the flow chart of the security system operation. As the system is automated so once the system is powered ON, then no need to human help to operate. After turning on, the Arduino waits in a loop for 'getting signal from sensors. If Arduino gets signal from any sensors then it creates an alarm and also send a warning message to the dedicated phone via GSM modem.

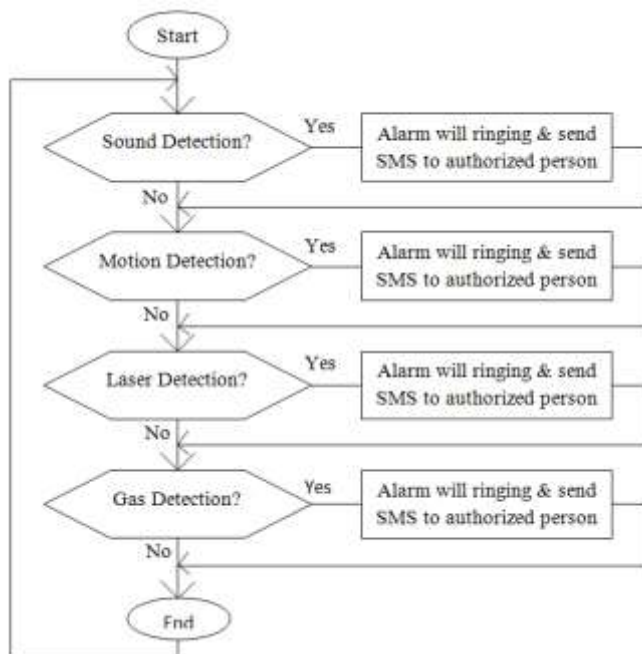


Figure 3. Flow Chart of System Operation

From the flow chart, when Sound sensor detects any kind of sound inside or in front of the bank vault and immediately a warning alarm ringing and GSM module sends a message to the authorized person.

If any object inside the Bank Vault is moving then the motion sensor immediately detect it and also alarming us by alarm & SMS.

From figure 2, Laser ray is reflected by the mirror and surrounded the Bank Vault. Laser ray is invisible in open eye, as a result, when an unauthorized person tried to come close to the vault, then the laser ray will be interrupted and Laser sensor suddenly sends a signal to the Arduino, also alarming us by alarm & SMS.

When someone leak Gas inside the vault room, Gas sensor will detect the leakage of gas and immediately alarming us through alarm and warning SMS. Bank vault can be Monitored remotely from anywhere in the world through IP camera.



Figure 4. Design Implementation

V. RESULTS AND DISCUSSION

The existing security system suffers with different problems. The proposed Bank Vault security system overcomes all of them.

TABLE I. COMPARATIVE STUDY BETWEEN PRESENT AND PROPOSED BANK VAULT SECURITY SYSTEM

S.No.	Present System	Proposed System
1	In existing system, use analog security lock in the vault room door.	In the proposed system, an integrated security system has been used in the vault room.
2	Use ordinary CCTV camera.	Used IP Camera so that vault room can monitor from different places.
3	Don't use laser technology.	Laser technology has been used.
4	Never use sound sensor.	Used Sound sensor.
5	Never use motion detector.	Motion detector has been used.
6	Don't use automated security system	The proposed security system is Fully automated.
7	Never use GSM technology	Used GSM technology

VI. CONCLUSION

In this paper, secure, automated, remote monitoring solution for Bank Vault has been presented. The approach discussed in the paper is novel and has attained the target to secure Vault room using the GSM-based security system satisfying needs and demands. Hence it can be concluded that the proposed security system has been achieved required goals and objectives. This project has been completed, tested several times and found working fine. In a near future, the number of security levels can be increased by using different sensors and other security equipments. This Proposed security system can also be used in other highly restricted areas such as offices, homes, Laboratories etc.

ACKNOWLEDGEMENT

The authors would like to express their sincere thanks to Faculty of Engineering, University Of Development Alternative (UODA) for providing help till the completion of the work.

REFERENCES

- [1] N. Khera, A. Verma, "Development of an Intelligent System for Bank Security", Deptt. Of ECE, Amity Univ., Noida, India, *Confluence The Next Generation Information Technology Summit (Confluence)*, 2014 5th International Conference, pp. 319-322, 25-26 September 2014.
- [2] A. Verma, "A Multi Layer Bank Security System", ECE Department, ASET, Noida (U.P.), 201301, India, *Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013 International Conference on, pp. 914-917, 12-14 December 2013.
- [3] "Arduino UNO", Arduino. cc/en. Retrieved 21 January 2016.
- [4] "SIM900 GPRS/GSM Shield", linksprite.com. Retrieved 21 January 2016.
- [5] "How Lasers Work", lasertech.com. Retrieved 21 January 2016

- [6] Gas sensor "MQ-5 datasheet", parallax.com. Retrieved 13 January 2016.
- [7] "How Infrared motion detector components work", *Noncommercial research page*, glolab.com. Retrieved 21 January 2016.
- [8] "How does a sound sensor work?" ask.com. Retrieved 21 January 2016.
- [9] Alexandr Lytkin, "IP Video Surveillance. An Essential Guide", ISBN 978-5-600-00033-9, 2012.

AUTHORS PROFILE



Ripan Kumar Ray received his B.Sc. (Engg.) degree in Electronics and Telecommunication Engineering from University Of Development Alternative. His research interest includes Embedded System, Automation System, Security, Networking and Wireless Communication Systems.



Muhammad Afsar Uddin is currently serving as a Lecturer in the department of Computer Science & Engineering, University Of Development Alternative, Dhaka, Bangladesh. He received his B.Sc. (Engg.) degree in Computer Science and Telecommunication Engineering & M.Sc.(Engg.) in Telecommunication Engineering from the department of Computer Science and Telecommunication Engineering of Noakhali Science and Technology University, Noakhali, Bangladesh. His research interest includes Microstrip Patch Antenna, Wireless Communication Systems, Neural Networks, Security and Communication Protocol.



Syed Foysol Islam is currently serving as a Associate Professor, Department of CSE and ETE University of Development Alternative (UODA), Dhaka, Bangladesh. He received his B.Sc. (Engg.), M.Sc. (Engg.) degree in Computer Science from Rajshahi University, Bangladesh and M.Sc. (Engg.) in Electrical Engineering from BTH, Sweden. His research interest includes Wireless Communication Systems, Communication Protocol and Security.

Human Authentication based on Bioelectrical Signals

Nastaran Maus Esafahani, Parinaz Saadat

*Department of Computer Engineering, Amirkabir University of Technology, Iran University of Science and Technology
Tehran, Iran*

Abstract— Human authentication based on electrical bio-signals, or bioelectrical signals, is a rapidly growing research area due to increasing demand for defining the identity of a person, with high confidence, in numerous applications in our vastly interconnected society. Studies show that bioelectrical signals can be not only employed for diagnostic purposes in medicine, but also used in human authentication since they have unique features among individuals. This article reviews examples of applying bioelectrical signals like Electrocardiogram (ECG), Electroencephalogram (EEG) and Electrooculogram (EOG) in human authentication and, up-to-date research efforts in this field. Utilizing bioelectrical signals provides a novel approach to user authentication that contains all the crucial attributes of previous traditional authentication. The most significant reasons for deployment of electrical bio-signals in user authentication include their measurability, uniqueness, universality and resistance to spoofing, while other conventional biometrics like face shape, hand shape, fingerprint and voice can be artificially generated.

I. INTRODUCTION

Authentication is carried out in a wide range of areas of different levels of security and importance. Not having a comprehensive understanding of the requirements for authentication according to different circumstances, we use the same traditional authentication, either through an object like an ID card or via knowledge like passwords, for every situation. This is while new authentication methods have advanced even beyond using conventional biometrics, and are applying bio-electrical signals for authentication purposes. The recent studies have shown that bio-signals can provide human authentication with the resistance to fraudulent attacks since they have specific features that are unique among individuals. In this article we introduce bioelectrical signals and mention their advantage over other conventional biometrics. After that we review some researches that have been carried out in the field of applying Electrocardiogram (ECG), Electroencephalogram (EEG) and Electrooculogram (EOG) signals for human authentication.

II. WHAT ARE BIOELECTRICAL SIGNALS?

Bio-signals are records of a biological event such as a beating heart or a contracting muscle. The electrical, chemical, and mechanical activity that happens during these biological

events often produces signals that can be measured and analysed [4]. Bio-signals are divided into six groups according to their physiological origin: bioelectrical signals, bio-magnetic signals, bio-chemical signals, bio-mechanical signals, bio-aquatic signals and bio-optical signals. The bio-signal of our interest in this article is bioelectrical signals. Bioelectrical signals are those that are generated by the summation of electrical potential differences across an organ [3]. Through surface electrodes either attached or close to the body surface, signals from a broad range of sources can be recorded [2]. Precisely, If a nerve or muscle cell is stimulated, it will produce an action potential that can be transmitted from one cell to nearby cells via its axon. When many cells become activated, an electric field is generated. These changes in potential can be measured on the surface of the tissue or organism by using surface electrodes [4]. Bioelectrical signals are very low amplitude and low frequency electrical signals [1]. These signals are generally used for medical diagnosis, but research findings confirm that since they have unique features among individuals, they can also be used for human authentication. The examples of bioelectrical signals are Electrocardiogram (ECG), Electroencephalogram (EEG), Galvanic skin response (GSR) and Electrooculogram (EOG) Fig.1.

III. THE ADVANTAGE OF BIOELECTRICAL SIGNALS OVER CONVENTIONAL BIOMETRICS

Biometric authentication systems use different physical or behavioural characteristics, for example, fingerprint, face shape, iris, hand geometry and voice pattern of an individual to define identity. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password [5]. Although this conventional biometrics is unique identifiers, they are not confidential and neither private to an individual since people put biometric traces anywhere. So, the original biometrics can be easily obtained without the permission of the owner of that biometrics. For example, in case of fingerprints, an artificial finger, known as gummy finger, can be made by pressing a live finger to plastic material, and then make an artificial finger with it or by capturing a fingerprint image from a residual fingerprint with a digital microscope, and then make a mould to produce an artificial finger [18]. In addition, thanks to the recent advances

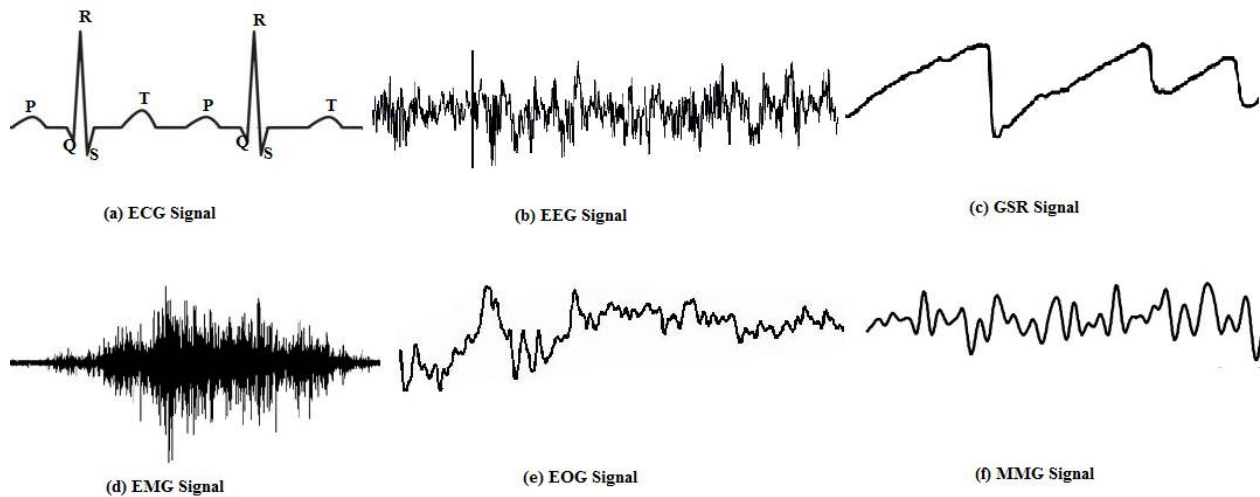


Fig.1. Bioelectrical signals [2]

in digital cameras and digital recording technologies, the acquisition and processing of high quality images and voice recordings has become a trivial task. Therefore, Iris scanners can be spoofed with a high resolution photograph of an iris held over a person's face [6]. The vulnerability of conventional biometrics to spoof has caused considerable concern especially in fields that require high reliable user authentication. This heightened concern leads to great interest in assessing the probability and efficiency of using bioelectrical signals in authentication systems. Using bioelectrical signals as biometrics offers several advantages. In addition to their uniqueness, bioelectrical signals are confidential and secure to an individual. They are difficult to mimic and hard to be copied. To be more precise, the biological information of a person is genetically governed from deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) proteins. Eventually, the proteins are responsible for the uniqueness in the certain body parts. Similarly, the organs like heart and brain are composed of protein tissues called myocardium and glial cells, respectively. Therefore, the electrical signals evoked from these organs show uniqueness among individuals [1]. So, by using bioelectrical signals as biometrics we can benefit from sufficiently invulnerable authentication systems.

IV. THE ELECTROENCEPHALOGRAPH SIGNAL AS A BIOMETRIC

As mentioned above the electroencephalogram (EEG) signal is one of the bioelectrical signals generated by brain activity, and can be recorded by positioning voltage sensitive electrodes on the surface of the scalp Fig.2. Typically, from 18 to 256 electrodes are placed on the scalp, each provides a time series sampled at 0.5-1.0 KHz, and generated hundreds of megabytes of data that must be analysed in order to extract useful information. The feature space of EEG data is very large coming from the fact that information is usually accumulated throughout parallel (across every single electrode) as well as considering that the human brain is really an

extremely complex dynamical system [12]. The EEG can reflect both the spontaneous activity of the brain with no specific task assigned to it, and the evoked potentials, which are the potentials evoked by the brain as a result of sensory stimulus [11]. EEG-based authentication has been studied nowadays and researches have demonstrated that the EEG brainwave signals could be used for individual authentication. These researches can be categorized into three groups based on the type of signal acquisition protocol used in authentication task and the mental state of the subject during signal acquisition [9]; EEG recordings while relaxation with closed or open eye; EEG recordings while being exposed to visual simulation; EEG recordings while performing mental tasks. The example of each category is explained below:

Qing Gui et al. [7] have presented an EEG-based biometric security framework. The data flow of authentication framework contained four steps. The first step was to collect raw EEG signals. 1.1 seconds of raw EEG signals was recorded from 6 midline electrode sites from 32 adult participants. Since it is argued that the brain activities are very focused during the visual stimulus process, the participants were asked to silently read an unconnected list of texts which included 75 words. In the next part, the noise level of raw EEG signals was reduced through ensemble averaging and low-pass filter. Ensemble averaging is a very effective and efficient technique in reducing noise because the standard deviation of noise after average is reduced by the square root of the number of measurements. After ensemble averaging, a 60 Hz low-pass filter was followed to remove the noise out of the major range of the EEG signals. In the third part, frequency features were extracted using wavelet packet decomposition. A wavelet is a mathematical function which can be used to divide a continuous-time signal into different scale component. A 4 level wavelet decomposition of the EEG signal after low pass filtering with 60 Hz was used to get the 5 EEG sub-bands, namely delta band (0-4 Hz), theta band (4-8 Hz), alpha band (8-15 Hz), beta band (15-30 Hz), and

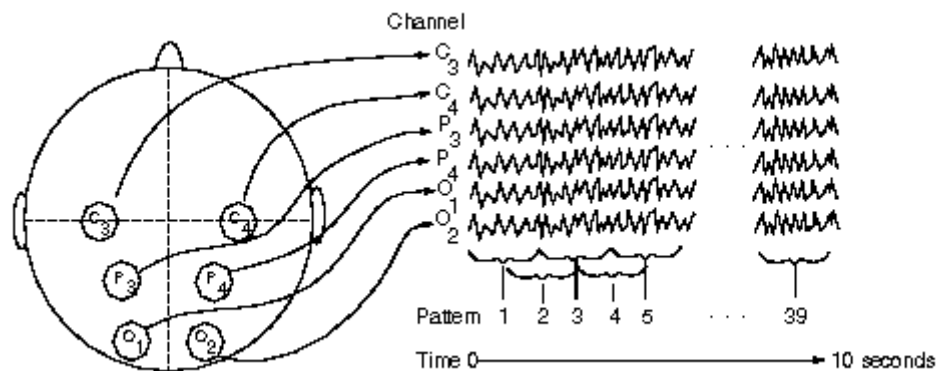


Fig.2. Signal acquisition (www.cs.colostate.edu)

gamma band. Since the energy distributions of the frequency components are quite different for each individual, it was possible to adopt those frequency components as the features to represent the EEG signals. The mean, standard deviation and entropy were also calculated to form the feature vectors. So, there were $3 \times 5 = 15$ features for each subject. Finally, in classification part, the input feature vector was compared to the feature vectors that have been stored in dataset to authenticate the identity of the subject.

Isao Nakanishi et al. [8] are also other researchers who have proposed new feature of EEG signals for authentication. They have used the concavity and convexity of spectral distribution in the alpha band of EEG signal in authentication to reduce the computational load for feature extraction, and authentication was done based on a linear combination of these features. They applied a consumer-use electroencephalograph that had only one electrode (single-channel) and was more convenient and practical compared to multi conventional channel measurements which increase the number of processing data, and require subjects to set a number of electrodes on the scalp. The single electrode was set on the frontal region of a head by using a head-band and subjects were asked to sit on a chair at rest with eye closed in quiet room that was the most suitable circumstances under which alpha wave can be detected. They adopted the spectrum analysis based on fast Fourier transform because it makes it easy to filter the spectrum in the alpha band and the concavity as well as the convexity of spectral distribution was used for distinguishing individuals. The concavity of spectral distribution was defined by detecting the maximum of the power spectrum and then calculating its tenth part and adopting it as a criterion. Then, frequencies of which power spectral values that were under the criterion were squared and summed. In addition to the concavity, the convexity of spectral distribution was another important feature. To define the convexity of spectral distribution the power spectral values in the alpha band were ranked and then the values and the frequencies of the top three were averaged. Next, the spectral values, which were greater than the averaged power spectrum, were summed. These three obtained features were as features which represent the convexity in spectral distribution. Finally,

the subject authentication was done according to some calculation on combination of these obtained features.

Another research has been carried out by S.Liu et al. [10]. They recruited twenty right-handed subjects with normal or corrected-to-normal visual acuity and 64-channels EEG signals were recorded continuously by electrodes that were placed on the scalp. Two hundred and sixty colour pictures were presented to the subject on a computer monitor located 1m away from him. Stimulus duration of each picture was 3s and all pictures were common and meaningful, identified and named easily. To find out suitable EEG features, several methods were employed to extract the EEG biometric features, including AR model, one of the most popular algorithms of feature extraction in which the series are estimated by a linear difference equation in time domain, power spectrum of the time-domain analysis that provides basic information of how the power distributes as a function of time, power spectrum of the frequency-domain analysis that provides basic information of how the power distributes as a function of frequency and phase-locking value which is a method to describe the synchronism between two signals. Then, all of the above-mentioned features were given to a support vector machine for classification respectively.

V. THE ELECTROCARDIOGRAM AS A BIOMETRIC

The heart makes use of electrical activity to activate the muscles required to pump blood through the circulatory system. By laying sensitive recording electrodes at certain regions around the heart, the signals can be recognized. The signals generated by the heart beat forms a regular pattern that records the electrical activity of the heart [12]. This signal is known as Electrocardiogram and can be used in human authentication. Recent works in the ECG biometric recognition field can be categorized as either fiducial point dependent or independent. Fiducials are specific points of interest on the ECG heart beat, namely, P, QRS and T waves that are shown in Fig.3. By using these features a reference vector is produced to use for authentication.

Steven A. Israel et al. [13] have shown that ECG attributes are unique to each individual and can be used in human

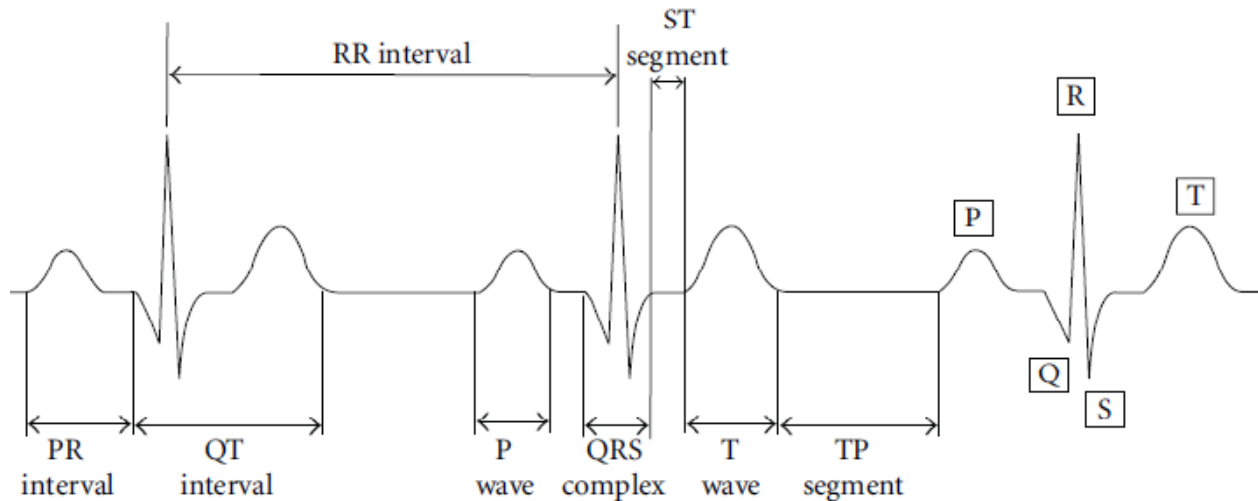


Fig 3. The typical ECG signals that include three heartbeats [4]

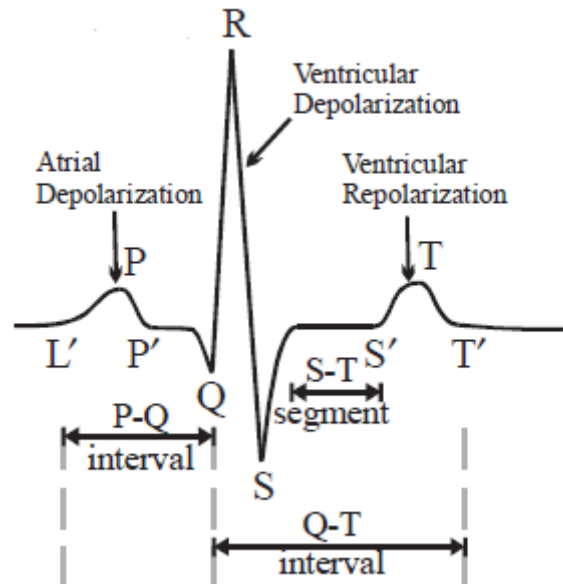


Fig 4. The fiducial points' physical positions [14]

authentication. In their experimentation, data were collected at high temporal resolution from twenty nine individuals. At first step, a filter was designed and used to extract ideal data from raw ECG data and to locate fiducial positions by removing non-signal artefacts. The raw data contained both low and high frequency noise components associated with changes in baseline electrical potential of the device and the digitization of the analog potential signal respectively. After applying filtering, the ECG trace fiducial positions were located. For human identification, attributes were extracted from the P, R, and T complexes and four additional fiducial points which were named L', P', S' and T'. Physically, the L' and P' fiducials indicate the start and end of the atrial depolarization and S' and T' positions indicate the start and end of ventricular depolarization Fig.4.

Attributes that show the unique physiology of an individual were extracted by calculating the distance among the ECG fiducials. Classification was performed on heartbeats using standard linear discriminate analysis. A conversion was required to link the performance of the heartbeat classification to human identification. Standard, majority and voting were used to assign individuals to heartbeat data. The conversion was performed using contingency matrix analysis. Steven A. Israel et al. also demonstrated that the extracted features are independent of sensor location by collecting ECG data at two electrode placements, one at the base of the neck and another one at fifth intercostals spacing. After testing they found a strong agreement between neck and chest ECG data which proved that the extracted ECG attributes are independent of

sensor location. In addition, they proved that ECG attributes invariant to the individual's state of anxiety.

Monalisa Dey et al. [14] also used ECG as a biometric feature to authenticate a person. They generated an ECG feature matrix by using the features extracted from ECG, namely the time durations for the R-R, S-S, Q-Q, T-T, P-R, Q-T, and QRS intervals. Then, an inner product was performed between this feature matrix and a constant matrix. The product is then compared with a previously set threshold. If the result lied above the threshold, a binary value of 1 was assigned to it; otherwise 0. The combination of 1 and 0 produced the ECG-Hash code. After that, another ECG-Hash code was generated by using the original feature matrices and constant matrices in the same way as mentioned above. A matching was performed between these two ECG-Hash codes. On the event of a match, the individual was authenticated. Else, the authentication procedure failed.

Andre Cigaro Matos et al. [15] are other researchers that applied ECG as a biometric for human authentication by using the "the off-the-person approach". In this approach, as opposed to common ECG-based biometric systems that collects data by placing sensors on chest area, the ECG were acquired at the fingers with dry Ag/AgCl electrodes, and using a custom ECG sensor which consists of a differential sensor design with virtual ground when subjects were at resting situation. Then features were extracted based on a frequency approach and was based on Odinaka algorithm in which a single heart beat was divided into 64ms windows, the analysis was performed in the frequency domain, computing the short time Fourier transform for each window. Finally a matching was performed on extracted features to do authentication.

VI. THE ELECTROOCULOGRAM AS A BIOMETRIC

There are different types of eye movements like saccade and smooth pursuit which comprise enough information to human authentication, and among them saccade is the most popular and simplest for biometric authentication. According to measurement method, eye movement signals can be divided into two groups: electrooculographical and videooculographical [3]. In Electrooculography the cornea-retinal potential that exists between the front and the back of the human eye is measured by placing electrodes left and right or top and above eye, and in video oculography the horizontal, vertical and torsional position components of the movements of both eyes are recorded by small cameras. Compared to other bioelectrical signals, fewer researches have been carried out in the field of applying eye oriented bioelectrical signals in human authentication.

One of these few researches has been carried out by M. Abo-Zahhed et al. [16]. They have proposed a new biometric authentication based on the eye blinking waveform and used the Neurosky Mindwave wireless headset to collect the raw eye blinking signal of 25 healthy subjects. The headset is actually for recording EEG signals, but by placing the armed sensor which is made of dry electrode on forehead above the eye; it can be used to measuring EOG signals. Each subject was asked not to do any eye movement, and to make 8-12 eye

blinks when signal recording was performing in quiet and normal temperature environment at daylight. The first step was isolating EOG signal from EEG signal through the technique of Empirical Mode Decomposition. Precisely, the raw EEG signal was decomposed into Intrinsic Mode Functions and after analysing them, it was found that the first two IMFs belonged to EEG and others were related to EOG signals. After this step, eye blinking signal was extracted from EOG signal with the help of its largest amplitude in EOG signal. Then, a certain threshold was adopted to detect the positive and negative peaks of the eye blink. The next step was feature extraction and four groups of features were extracted based on time delineation of the eye blinking waveform and its derivatives Fig.5. Amplitude of positive peak of eye blink, area under positive pulse of eye blink, slope at the onset of positive pulse and position of positive peak of first derivative of eye blinking signal are one sample of each group. To evaluate the performance of system, the proposed system was tested under each four group of features, and based on achieving results, M. Abo-Zahhed et al. came to conclusion that the group of feature which was including area under positive pulse of eye blink, area under negative pulse of eye blink, energy of the positive pulse of eye blink, energy of the negative pulse of eye blink, average value of positive pulse of eye blink and average value of negative pulse of eye blink was the best for authentication of the subjects.

M. Juhola et al. [17] also have introduced a method in which a subject's saccade was applied to authentication. From their point of view, saccades are easy to stimulate and natural while reading or looking at the surroundings all the time. They decreased data for authentication process by using only the saccades parts of eye movements' signals.

They asked each subject to sit down at a computer and the computer system had to verify him or her to be or not to be the authenticated subject. The system consisted of a device able to detect a subject's saccades and a program that computed features from saccades. They employed two small video cameras, one for each eye, to follow the pupils of a subject's eyes. Every subject was seated in chair at a fixed location and with the same distance from the stimulation device and was due to look at a small, horizontally jumping target and his or her eye movements were recorded for the authentication purpose. Signals given by this video-oculography system could be typically measured with a low sampling frequency, in this case with 30 Hz. After the recognition of every valid saccade, its amplitude, accuracy, latency and maximum velocity were computed to be used in authentication process Fig.6.

Latency is the time difference between the beginnings of the stimulus movement and response, accuracy is equal to the difference of the amplitudes of the stimulation and saccade and to compute the maximum angular velocity, the first derivative was approximated by differentiating an eye movement signal numerically and searching for the maximum velocity during the eye movement. They took these four particularly after having observed how clearly they varied between individuals. In addition, they applied EOG signal to

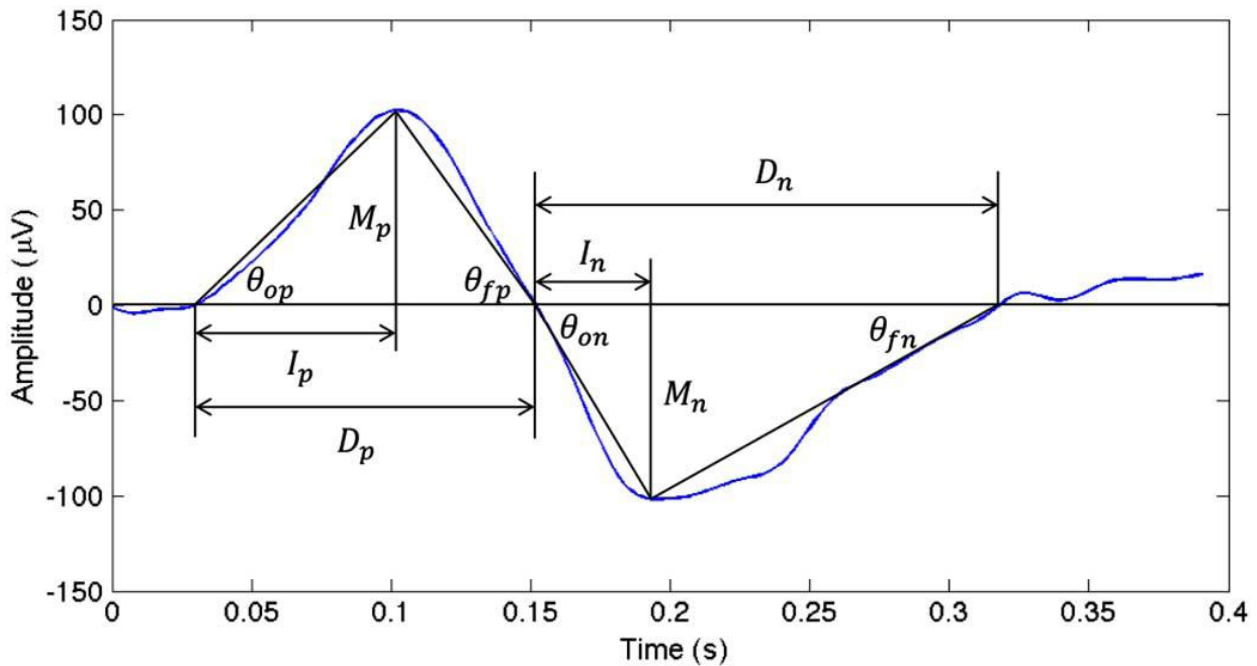


Fig 5. Features extracted from the eye blinking

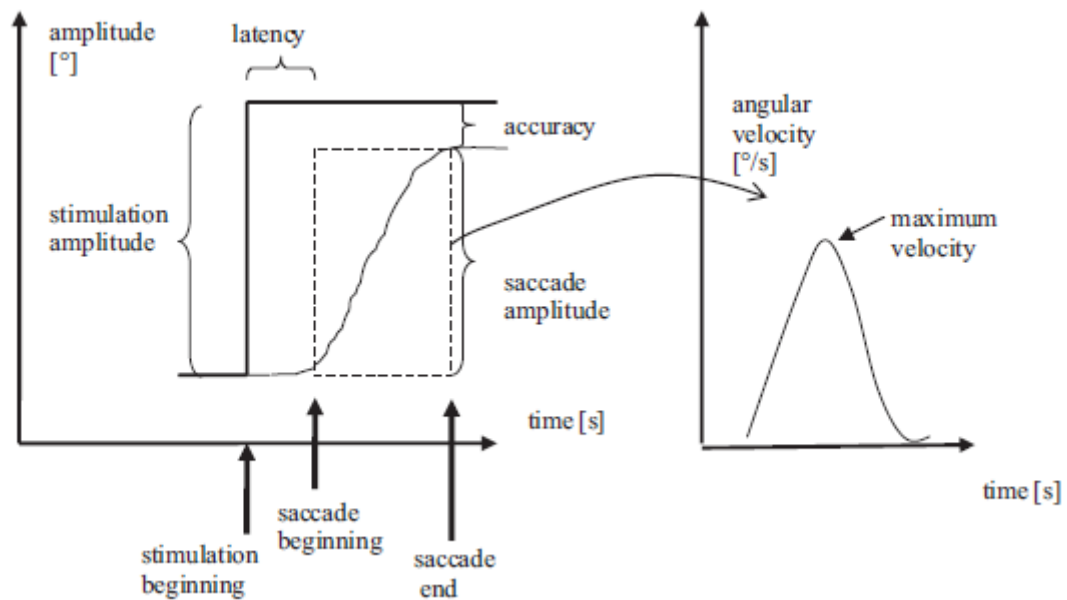


Fig 6. An ideal saccade as a response to stimulation [17]

user authentication and although the VOG signals contained less noise than the EOG signals, in most situations the EOG measurements achieved better results on the average than the VOG measurements. They supposed that the higher original sampling frequency of the EOG signals leads to better authentication results.

VII. CONCLUSION AND DISCUSSION

This article has presented some of researches that have been carried out in the field of applying bioelectrical signals in human authentication. All of these researches agree that each

bioelectrical signal has its own confidential physiological features which cannot be mimic and stolen. So, through these highly secured features, bioelectrical signals offer more advantage compared with conventional biometrics like fingerprint or iris for human authentication. But there are some issues and challenges involved in applying bioelectrical signals as biometrics. Firstly, all of mentioned researches have been done under laboratory condition with limited subjects. Therefore, the performance of bioelectrical -signal based authentication system might decline in practical real condition with more subjects. secondly, the data acquisition of

bioelectrical signals is a challenging activity, as explained before, measurement of ECG signals with good quality requires skin electrodes attached to the certain locations of the chest or EEG signals can be recorded by placing some electrodes over the scalp and the placement of electrodes to right position may cause distortion in the recorded signal. So, the data acquisition of bioelectrical signals could be an obstacle in applying these signals to human authentication in non-laboratory condition. Lastly, it should be considered that bioelectrical signals might be dependent to the mental and emotional state of subject. For example, fatigue, alcohol and aging could affect EOG signals, or EEG and ECG signals might vary with stress and anxiety.

REFERENCES

- [1] Enderle, J. D., & Bronzino, J. D. (2012). Introduction to biomedical engineering. Academic press.
- [2] Pal, A., Gautam, A. K., & Singh, Y. N. (2015). Evaluation of Bioelectric Signals for Human Recognition. *Procedia Computer Science*, 48, 747-753.
- [3] Van Den Broek, E. L., & Spitters, M. (2013). Physiological signals: The next generation authentication and identification methods!?. In *Intelligence and Security Informatics Conference (EISIC), 2013 European* (pp. 159-162). IEEE
- [4] Singh, Y. N., Singh, S. K., & Ray, A. K. (2012). Bioelectrical signals as emerging biometrics: Issues and challenges. *ISRN Signal Processing*, 2012.
- [5] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media.
- [6] Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging 2002* (pp. 275-289). International Society for Optics and Photonics
- [7] Roberts, C. (2007). Biometric attack vectors and defences. *Computers & Security*, 26(1), 14-25.
- [8] Revett, K., Deravi, F., & Sirlantzis, K. (2010). Biosignals for user authentication-towards cognitive biometrics?. In *Emerging Security Technologies (EST), 2010 International Conference on* (pp. 71-76). IEEE.
- [9] Hadjileontiadis, L. J. (2006). Biosignals and compression standards. In *M-Health* (pp. 277-292). Springer US.
- [10] Abo-Zahhad, M., Ahmed, S. M., & Abbas, S. N. (2015). A new multi-level approach to EEG based human authentication using eye blinking. *Pattern Recognition Letters*.
- [11] Gui, Q., Jin, Z., & Xu, W. (2014). Exploring EEG-based biometrics for user identification and authentication. In *Signal Processing in Medicine and Biology Symposium (SPMB), 2014 IEEE* (pp. 1-6). IEEE.
- [12] Nakanishi, I., Baba, S., & Miyamoto, C. (2009). EEG based biometric authentication using new spectral features. In *Intelligent Signal Processing and Communication Systems, 2009. ISPACS 2009. International Symposium on* (pp. 651-654). IEEE.
- [13] Liu, S., Bai, Y., Liu, J., Qi, H., Li, P., Zhao, X., ... & Li, Q. (2014). Individual feature extraction and identification on EEG signals in relax and visual evoked tasks. In *Biomedical Informatics and Technology* (pp. 305-318). Springer Berlin Heidelberg.
- [14] Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., & Wiederhold, B. K. (2005). ECG to identify individuals. *Pattern recognition*, 38(1), 133-142.
- [15] Dey, M., Dey, N., Mahata, S. K., Chakraborty, S., Acharjee, S., & Das, A. (2014). Electrocardiogram Feature based Inter-human Biometric Authentication System. In *Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on* (pp. 300-304). IEEE.
- [16] Matos, A. C., Lourenço, A., & Nascimento, J. (2014). Embedded System for Individual Recognition Based on ECG Biometrics. *Procedia Technology*, 17, 265-272.
- [17] Abo-Zahhad, M., Ahmed, S. M., & Abbas, S. N. (2015). A novel biometric approach for human identification and verification using eye blinking signal. *Signal Processing Letters, IEEE*, 22(7), 876-880.
- [18] Juhola, M., Zhang, Y., & Rasku, J. (2013). Biometric verification of a subject through eye movements. *Computers in biology and medicine*, 43(1), 42-50.

Customer Relations Management using J48 Tree, Ranking Algorithm, and Chi-Square

Marzieh mohammadi
Faculty of Computer Engineering,
Institution. in Proc, Islamic Azad
University, Isfahan, Iran

Hamid Rastegari
Faculty of Computer Engineering,
Najafabad branch, Islamic Azad
University, Isfahan, Iran

Abstract— Customer relations management (CRM) integrates all business activities to identify and manage customers in order to increase sales in the long run and thus raise the value of companies. Efficient administration of CRM requires the recognition of appropriate patterns within the existing datasets. Analysis of such patterns will then enable managers and analysts to make the best possible decisions in critical situations. Pattern recognition is one of the fundamental goals of data mining techniques. Decision trees are popular data mining approaches commonly used as prediction models. The present study proposed a model which utilized both classification (based on J48 tree) and feature selection for the accurate prediction of marketing performance. The efficacy of the proposed model was evaluated in three datasets and the results were compared with other widely used data mining algorithms including the reduced-error pruning (REP) tree, random decision tree, support vector machine (SVM), and J48 tree. The results confirmed the higher precision, accuracy, and recall and lower error rate of the proposed model compared to the other four methods.

Keywords- Customer Relations Management (CRM); Feature Selection; Data mining; Classification; J48 Tree; Ranker Algorithm; Chi-square

I. INTRODUCTION

Customer relationship management (CRM) involves a series of processes and technologies utilized by companies to identify and attract potential customers, expand their customer base, provide higher quality services, and ultimately retain customers. CRM principles discuss the

methods of successful establishment, implementation, and maintenance of an efficient customer relationship system [1]. As an integrated information system, a CRM system seeks to improve customers' experiences of interaction with a corporate by using an assortment of channels (e.g. corporate's website, email, and telephone) to organize, schedule, and control pre- and post-sale activities. In other words, in its attempt to increase profitability, revenue, and customer satisfaction, a CRM (as a grand strategy) organizes business activities based on different groups of customers and tries to create and promote particular behaviors which can eventually promote customer satisfaction [2]. Such a system will help businesses not only to retain current customers, but also to acquire new groups of customers. Organizations may adopt various methods, including CRM, customer value analysis, and organizational and service provision strategies, to enhance the efficiency of customer relationships and thus attract and retain new customers. CRM can be applied to monitor all activities related to direct customers (e.g. firms), shorten the sales cycle, improve customer loyalty, and increase profit [3].

Data mining is a commonly used approach to manage, organize, and discover predictive patterns existing in a large dataset without the need to involve users. It employs several techniques, such as preprocessing, classification, clustering, and feature selection, and algorithms to provide managers and analysts with the information required for decision-making in critical organizational situations [4]. Identification

of customer needs using data mining methods will enable businesses to tailor their services based on the obtained patterns and available information about products, customers, and their interests. Therefore, the relationship between data mining and CRM can play a major role in the success of organizations. A previous study proposed the application of decision trees for the identification and prediction of changes in marketing and sales trends. After evaluating the approach using a dataset extracted from an online shopping website in Korea, the model was found to be capable of helping managers to make appropriate decisions based on customer needs and requests [5].

Decisions trees are one of the oldest and most popular data mining techniques. They generally perform classification by predicting an analog output based on categorical or actual inputs. Owing to their ability to comprehensively describe the relations within a dataset, decision trees are widely used for classification and prediction purposes in a variety of fields (e.g. marketing) [6]. Since the decision tree (algorithm output) is generated based on the values of a set of selected features, the accuracy of a pattern recognition system largely depends on appropriate feature selection. On the other hand, as higher numbers of features impose additional computational costs on the system, design and implementation of systems with the minimum possible number of features seems essential. Feature selection, i.e. choosing the optimal (or suboptimal) subset of features in the dataset, aims to reduce the decision tree size without decreasing classification accuracy. It is hence crucial to pattern recognition, machine learning, and data mining [7].

The present study applied J48 and ranking algorithms to develop a decision tree for predicting customer behavior and selecting the set of activities that can potentially increase profitability. Chi-square tests were performed for data analysis. The proposed model was then compared with several other data mining algorithms including reduced-error pruning (REP) decision trees, random decision trees (RDT), support vector machines (SVM), and J48 tree. Ross Quinlan

introduced C4.5 as an algorithm to create decision trees from a set of labeled training data [8]. Weka open source data mining software incorporates J48 algorithm as an implementation of C4.5.

II. CONCEPTS AND RELATED WORK

A. Concepts

1) Rep tree

Rep Tree are simple and fast decision trees. After building a tree by using information gain as the splitting criterion, REP is applied to prune the created tree [9,10]. This algorithm sorts values for numeric features only once and handles missing values according to C4.5 for fractional instances [10].

2) Random tree

RDTs are increasingly used as an efficient method in the field of data mining. An RDT is basically created by selecting a random feature at each node. These trees are usually left unpruned and are considered as control trees [9,10]. The general belief is that producing a large group of RDTs can ensure accuracy while preventing the problem of overfitting. Due to random selection of the features, all trees of the group will have equal chance of being sampled [10].

3) SVM

SVM is a kernel method originally developed by Vapnik (1992) based on the probability theory in machine learning [11]. SVM owes its popularity to its accuracy in handwriting recognition (which is equal to that of neural networks). While SVM algorithms have been widely used in various applications, only two instances of them have been applied in direct marketing.

SVM algorithms use clustering, classification, ranking, and data cleaning to recognize complex patterns in a dataset. While these algorithms are highly efficient in some applications, computational complications decrease their efficiency in dealing with large datasets [12,13]. Therefore, SVM classifiers are suitable when the training data have limited features.

4) Feature Selection

Feature selection techniques are commonly applied in data mining practices to identify and eliminate irrelevant or redundant data and thus reduce dataset size while maintaining the accuracy of predictive models [14]. Such a reduction in the number of features will decrease the complexity and improve the cost-effectiveness, speed, and performance of predictive models [15]. Feature selection techniques can be categorized as filter methods (e.g. chi-square test, information gain, and correlation coefficient scores), wrapper methods (e.g. random hill-climbing algorithm and forward selection and backward elimination), and embedded methods [e.g. regularization techniques such as the least absolute shrinkage and selection operator (LASSO), elastic net, and ridge regression].

B. Related Work

Numerous studies have assessed the applicability of various data mining methods in different fields of business [16]. Previous research has also focused on appropriate intelligent data mining methods to improve CRM [17-18]. Several techniques including association rules, clustering, classification, and sequence discovery have been adopted to deal with customer complaint and loyalty issues (as components of CRM) and enhance customer retention. Any classification method in data mining comprises a learning phase (during which a classifier is produced by using a predefined set of data classes) and the actual classification phase [19].

In business studies, decision trees are widely used to predict future customer behaviors and describe sequences of interrelated decisions based on patterns extracted from available customer data [1,20,21]. Kim et al. proposed a decision tree-based method and evaluated its efficacy using a Korean online shopping center. They concluded that the method could detect changes in customer behaviors not only in structured situations (where the manager was interested in a specific research matter), but also under dynamic conditions [21]. Bin et al. tried to develop an accurate and efficient model based on decision trees to predict customer churn among Personal Handyphone System Service users. They performed three experiments to construct an accurate and effective customer churn model and reported the optimal model to use random sampling for training set selection, a sub-period time of 10 days, and a misclassification rate of 1:5 [22].

III. THE PROPOSED MODEL

Data mining techniques are widely employed to create frameworks covering all aspects of CRM [16]. Such a process comprises four stages. First, the problem has to be analyzed. The identification of hidden patterns in customer behaviors during this stage will facilitate decision making for business managers. In the next stage, i.e. data preparation

stage, the required data should be collected from different sources and issues related to missing data and outliers should be carefully dealt with. The prepared data will be used in the third stage to build an appropriate model for CRM. In the final stage, the developed model is validated to ensure its applicability in CRM [10]. In the present study, a model based on J48 decision tree is proposed. We believe that the model should have a high accuracy in making predictions in the field of CRM. The proposed model will involve three phases including preprocessing, feature selection, and classification with J48 tree (Figure 1).

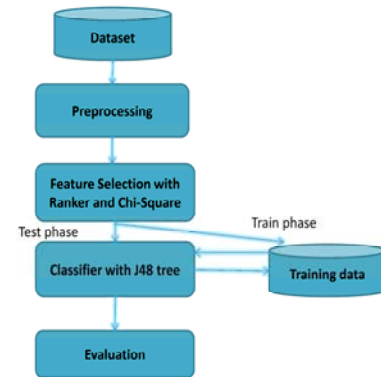


Figure 1: The proposed model

A. Preprocessing phase

Since data preparation and filtering can potentially be very time-consuming, data pre-processing, including normalization, cleaning, transformation procedures [23], is identified as a critical stage of all data mining processes. Normalization (e.g. rescaling) is an essential data preprocessing approach [14] with well-known benefits for prediction purposes [24]. The existing normalization methods, such as min-max, z-score, and decimal scaling, are commonly applied to scale different parameters into the same range and thus eliminate the variations in predictions. Our proposed model uses z-scores to normalize unstructured data during the preprocessing phase:

$$V_i' = \frac{V_i - E}{\text{std}(E)} \quad (1)$$

where V_i' is the z-score normalized value and V_i is the value in row E and the i^{th} column. If there are five rows (V-Z) each containing n columns (or variables), then:

$$\text{Std}(E) = \sqrt{\frac{1}{(n-1)} \sum_{i=1}^n (v_i - \bar{E})^2} \quad (2)$$

$$\bar{E} = \frac{1}{n} \sum_{i=1}^n v_i \text{ or mean value}$$

The above-mentioned equations can be used to calculate normalized values in each row. When all values in a particular row are identical, the standard deviation of that row, and thus all the normalized values in that row, will be equal to zero.

B. Feature selection with a Ranker and Chi Square Test

Among the various feature selection methods, ranking approached are used to categorize disorganized groups of data based on ranks allocated to each item according to one or more of its features. Rankings are applied for prioritizing tasks or comparing the performance of different products. Although rankings can be easily visualized, the interpretation of the obtained visualizations might be tricky since the rank of a particular object may not fully describe the complicated relations between its features and attributes of other objects. In fact, since numerous rankings can be developed within a specific setting, their comparison is essential to determine the effects of heterogeneous features on each ranking. Moreover, the efficiency of this process needs to be enhanced through the application of advanced visual examinations [25]. Ranking methods are usually in used in combination with techniques to determine feature significance (e.g. Relief-F, gain ratio, and entropy). In order to perform the ranking, a specific threshold is determined for the features and measures above this threshold are selected. A general algorithm will also be required to select one of the best ranking measures with the most suitable features from the classification point of view.

Chi-square test is a non-parametric (distribution-free) test widely employed to compare ratios, frequencies, and percentages in univariate or multivariate problems. This test was incorporated into our proposed model since its non-parametric nature allowed for undetermined parameters, null values, and missing, heterogeneous, and dispersed data.

In models developed by previous research [10, 25], a ranking algorithm is first applied to sort each feature. The ChangesSameValue function is then used to identify similar and different values for a particular feature and compute the maximum number of changed labels. In other words, this

function calculates the ranking of each feature as the number of changes in class labels. In our proposed model, the probability table for each feature is first developed based on the frequency of each value in each class. The expected values are then determined based on the probability of the incidence of each value in a specific class. In the next step, equation (3) is used to calculate chi-square from the values in the obtained probability table. Chi-square values for each feature are stored in the variable named NLC and the algorithm is repeated for all features. Ultimately, the values in the NLC are sorted. Figure 2 shows a pseudocode for the proposed method.

```

The Proposed Algorithm()
Input: E training(N instances, M features)
Output: E reduced(N instances, M ranker features)
For each feature  $A_i \in 1..M\{$ 
  (A) Expand the contingency table to have both row totals and
  column totals and an overall total.
  (B) Calculate the "expected values" for each cell in the table
  based on the probabilities using the totals of each row and
  column.
  (C)  $NLC_i \leftarrow$  Organize the frequencies into a new table to
  calculate  $X^2$ .
  That  $X^2(\text{features}) = \sum_{j=1}^M \frac{(f_o - f_e)^2}{f_e}$ 
}
Sort NLC Feature Ranking
Select the ranked feature

```

Figure 2: The pseudocode for the proposed method

Chi-square tests are applied to evaluate the features of each node. In fact, chi-square test is a statistical test which compares the occurrence of each feature with its expected occurrence in each class [26]. The independent and dependent variables in chi-square tests are features and classes, respectively. Chi-square value for a particular feature can be calculated as [27]:

$$X^2(\text{features}) = \sum_{j=1}^M \frac{(f_o - f_e)^2}{f_e} \quad (3)$$

where f_o and f_e are respectively the observed and expected occurrences of the feature in a particular class. M is the number of features. Figure 3. The flowchart of the pseudocode for the proposed feature selection approach

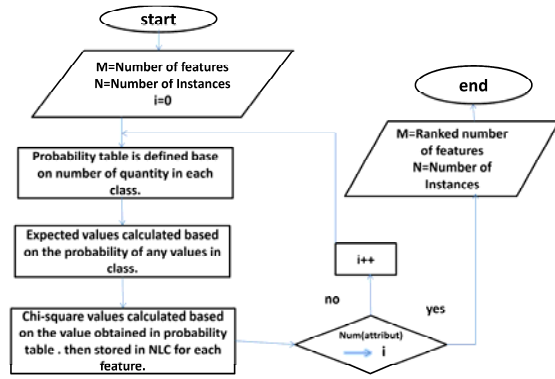


Figure 2: The pseudocode for the proposed feature selection approach

C. Classifier phase with J48 tree

As an implementation of C4.5, the J48 decision tree is popular in data mining applications [14]. Since decision trees created by C4.5 can be employed for classification purposes, they are also known as statistical classifiers [9]. The J48 is a pruned tree which considers all possible tests for the classification of features and selects the best test outputs based on entropy and chi-square techniques. Three steps are generally followed to produce a J48 tree:

- When all instances belong to the same class, the tree will have a leaf labeled with the mentioned class.
- A test is performed on the feature and the possible information for each feature is obtained. The information gain is then calculated accordingly. During this stage, entropy is used as an indicator of data disorder:

$$\text{Entropy}(\bar{y}) = -\sum_{j=1}^J \frac{|j|}{|S|} \log\left(\frac{|j|}{|S|}\right) \quad (4)$$

$$\text{Entropy}(j|\bar{y}) = \frac{|j|}{|S|} \log\left(\frac{|j|}{|S|}\right)$$

Information gain can thus be computed as:

$$\text{Gain}(\bar{y}, j) = \text{Entropy}(\bar{y}) - \text{Entropy}(j|\bar{y}) \quad (5)$$

- Finally, the best feature is selected based on the present selection measure and that feature selected for branching [26].

IV. RESULTS AND DISCUSSION

The proposed model was validated by its administration on three experimental datasets including Bank-Data.csv¹, Car.arff², and Bank-full.csv³ (Table 1). Precision, accuracy, recall, and error rate were computed with 10-fold cross-validation (equations 6-9).

$$\text{Precision} = \text{TP}/(\text{TP}+\text{FP}) \quad (6)$$

$$\text{Accuracy} = (\text{TP}+\text{TN})/\text{N} \quad (7)$$

$$\text{Recall} = \text{TP}/(\text{TP}+\text{FN}) \quad (8)$$

$$\text{Error rate} = (\text{FN}+\text{FP})/\text{N} \quad (9)$$

where TP is the number of features correctly identified by the classifier; FP is the number of features incorrectly identified by the classifier; TN is the numbers of features correctly rejected by the classifier; FN is the number of features incorrectly rejected by the classifier; and N is the number of features.

Table 1 The used datasets:

TABLE I. DATASET IN USE

Dataset	Number of Instances	Number of Features
Bank-Data.arff	600	16
Bank-full.arff	41189	21
Car.arff	1727	7

The results of the proposed model were compared with those of REP tree, RDT, SVM, and J48 tree. The proposed model was implemented by java Net Beans and the .jar files from WEKA were imported into the source code. All experiments were executed on a computer system with a Core i7 CPU and 8 GB of RAM.

Tables 2 and 3 compare the precision and recall of the proposed model with that of the REP tree, RDT, SVM, and J48 tree. As seen, in all datasets, the use of data normalization and feature ranking by chi-square tests increased the precision and recall of the proposed model compared to the other three algorithms. The second highest precision and recall in all datasets belonged to the J48 tree algorithm which used entropy and all possible tests to identify the best branches and produce a pruned tree. Moreover, in Bank-full and Car datasets, the REP tree

¹

<http://facweb.cs.depaul.edu/mobasher/classes/ect584/WEKA/preprocess.html>

² <http://repository.seasr.org/Datasets/UCI/arff/>

³ <http://mlr.cs.umass.edu/ml/machine-learning-databases/00222/>

algorithm had higher precision and recall than the SVM and RDT algorithms. The RDT and REP tree algorithms had the lowest precision in the Bank-full and Bank-data datasets, respectively. Due to the absence of pruning in the RDT algorithm, this method had the lowest recall in both Bank-full and Car datasets. The REP tree algorithm had the lowest recall in the Bank-data dataset.

Table2. Comparison of the proposed model and the reduced-error pruning (REP) decision tree, random decision tree (RDT), support vector machine (SVM), and J48 tree in terms of precision.

TABLE II. THE COMPARISON OF PRECISION WITH REP TREE, RDT,SVM, J48 TREE AND PROPOSED MODEL

dataset	Rep tree	RDT	SVM	J48 tree	The Proposed model
Bank-full.arff	90.5	88.4	88.7	90.7	95.5
Bank-Data.arff	29.5	60.6	61.1	89.9	92.9
Car.arff	88.0	82.7	80.0	92.4	96.9

As it can be seen in table 2, the precision of proposed model is higher than the other algorithm. J48 tree is more precise than Rep tree and Random tree and Rep tree has the precise than Random tree because random tree is not pruning.

Table 3. Comparison of the proposed model and the reduced-error pruning (REP) decision tree, random decision tree (RDT), support vector machine (SVM), and J48 tree in terms of recall

TABLE III. THE COMPARISON OF RECALL WITH REP TREE, RDT, SVM, J48 TREE AND PROPOSED MODEL .

dataset	REP tree	RDT	SVM	J48 tree	The Proposed model
Bank-full.arff	91.1	88.6	90.3	91.2	95.7
Bank-Data.arff	54.3	58.0	61.3	89.8	92.7
Car.arff	87.7	83.2	84.7	92.4	96.8

Table 4 compares the accuracy of the proposed model with that of the REP tree, RDT, SVM, and J48 tree. Apparently, due to the above-mentioned reasons, the proposed model had the highest accuracy in all datasets. Furthermore, the J48 tree algorithm was the second most accurate method in all datasets. In the Bank-full and Car datasets, the REP tree had higher accuracy compared to the SVM and RDT algorithms.

Table 4. Comparison of the proposed model and the reduced-error pruning (REP) decision tree, random decision tree (RDT), support vector machine (SVM), and J48 tree in terms of accuracy

TABLE IV. THE COMPARISON OF ACCURACY WITH REP TREE, RDT, SVM, J48 TREE AND PROPOSED MODEL .

Dataset	REP tree	RDT	SVM	J48 tree	The proposed model
Bank-full.arff	91.1	88.6	90.3	91.2	95.7
Bank-Data.arff	54.3	58.0	61.3	89.8	92.7
Car.arff	87.7	83.2	84.7	92.4	96.8

Table 5 compares the four models in terms of error rate. As expected based on the obtained precision values, the lowest error rate (and thus the highest precision) in all datasets belonged to the proposed model. Data normalization during the preprocessing phase, feature selection, and elimination of redundant and irrelevant features can justify this finding. The second lowest error rate was detected in case of the SVM algorithm. Finally, the REP tree algorithm had a lower error rate than the RDT algorithm.

Table 5. Comparison of the proposed model and the reduced-error pruning (REP) decision tree, random decision tree (RDT), support vector machine (SVM), and J48 tree in terms of error rate

TABLE V. THE COMPARISON OF ERROR RATE WITH REP TREE, RDT, SVM, J48 TREE AND PROPOSED MODEL .

Dataset	REP tree	RDT	SVM	J48 tree	The Proposed model
Bank-full.arff	0.114	0.115	0.097	0.111	0.071
Bank-Data.arff	0.496	0.469	0.386	0.200	0.132
Car.arff	0.063	0.077	0.269	0.058	0.0174

V. CONCLUSION

Nowadays, many of companies spent a lot of money and time on the decisions for marketing their services and products and decision making by discovering interesting patterns in the amount of data has become a key task in today's business background. Generally, companies make a customer prediction model to discovery the prospects for a particular product. Data mining uses the algorithms to find useful patterns and trends from the extracted data so that it able to yield main insights including prediction models and associations can support companies understand their customer well. Analyzing and Examining data able to turn raw data into valuable information about customer's requires. Classifying and features selection are two main techniques of data mining. In this paper, a model base on the classification of J48 tree and feature selection with Ranker is proposed to predict precise marketing performance. The propose model is evaluated conducted 3datasets and the

results are compared with other algorithms such as Rep tree, Random tree and J48 tree. The experimental results show that the proposed model has higher precision and lower error rate in comparison of J48 tree, Rep tree and Random tree.

REFERENCES

- [1] Perreault Jr, W. D., E. J. McCarthy and J. P. Cannon ,Basic marketing: A marketing strategy planning approach, McGraw-Hill/Irwin, (2006).
- [2] Kostojohn, S., M. Johnson, and B. Paulen, Maintaining and Evolving CRM, in *CRM Fundamentals*. 2011, Springer. p. 197-224.
- [3] Jutla, D., J. Craig and P. Bodorik , Enabling and measuring electronic customer relationship management,(2001). *Proceeding of the 34th Annual Hawaii International Conference on*.2001.IEEE.
- [4] Linoff, G.S. and M.J. Berry, *Data mining techniques: for marketing, sales, and customer relationship management*. 2011: John Wiley & Sons.
- [5] Quinlan, J.R., *Induction of decision trees*. *Machine learning*, 1986. **1**(1): p. 81-106.
- [6] Kikuti, D., F. G. Cozman and R. Shirota Filho , Sequential decision making with partially ordered preferences, *Artificial Intelligence* (2011).175(7): p. 1346-1365.
- [7] Dash, M. and H. Liu, *Feature selection for classification*. *Intelligent data analysis*, 1997. **1**(1): p. 131-156.
- [8] Kim, J.K., et al., Detecting the change of customer behavior based on decision tree analysis. *Expert Systems*, 2005. **22**(4): p. 193-205.
- [9] Witten, I.H. and E. Frank, *Data Mining: Practical machine learning tools and techniques*. 2005: Morgan Kaufmann.
- [10] Mohammadi .M, H. Rastegari, Using J48 tree for value-based customer ralations management (CRM),2015vol.13 ,no.7 :p. 49-54.
- [11] Drucker, H.,S. Wu, and V.N. Vapnik, Support vector machines for spam categorization.*Neural Network,IEEE Transactions on*, 1999. 10(5): p. 1048-1054.
- [12] FENG, Y. and H. ZHOU, An Effective and Efficient Two-stage Dimensionality Reduction Algorithm for Content-based Spam Filtering* . *Journal of Computational Information System*, 2013. 9(4): p. 1407-1420.
- [13] Liu, H., J.Li, and L. Wong, A comparative study on feature selection and classification methods usinggene expression profiles and proteomic patterns. *Genome informatics*, 2002. 13:p. 51-60
- [14] Gholap, J., Performance tuning of J48 Algorithm for prediction of soil fertility. *arXiv preprint arXiv:1208.3943*, 2012.
- [15] Hall, M.A., *Correlation-based feature selection for machine learning*. 1999, The University of Waikato.
- [16] Ranjan, J. and V. Bhatnagar, Data mining tools: a CRM perspective. *International Journal of Electronic Customer Relationship Management*, 2008. **2**(4): p. 315-331.
- [17] Wong, K.W., et al. Intelligent data mining and personalisation for customer relationship management. in *Control, Automation, Robotics and Vision Conference*, 2004. ICARCV 2004 8th. 2004. IEEE.
- [18] Han, J., M. Kamber, and J. Pei, *Data mining: concepts and techniques: concepts and techniques*. 2011: Elsevier.
- [19] Ahmed, S.R. Applications of data mining in retail business. in *Information Technology: Coding and Computing*, 2004. *Proceedings. ITCC 2004. International Conference on*. 2004. IEEE.
- [20] Chen, Y.-L., C.-L. Hsu, and S.-C. Chou, Constructing a multi-valued and multi-labeled decision tree. *Expert Systems with Applications*, 2003. **25**(2): p. 199-209.
- [21] Kim, J.K., et al., Detecting the change of customer behavior based on decision tree analysis. *Expert Systems*, 2005. **22**(4): p. 193-205.
- [22] Bin, L., S. Peiji, and L. Juan. Customer churn prediction based on the decision tree in personal handyphone system service. in *Service Systems and Service Management*, 2007 *International Conference on*. 2007. IEEE.
- [23] Patro, S., et al., Technical Analysis on Financial Forecasting. *arXiv preprint arXiv:1503.03011*, 2015.
- [24] Gratzl, S., et al., Lineup: Visual analysis of multi-attribute rankings. *Visualization and Computer Graphics, IEEE Transactions on*, 2013. **19**(12): p. 2277-2286.
- [25] Ruiz, R., J.C. Riquelme, and J.S. Aguilar-Ruiz. Fast feature ranking algorithm. in *Knowledge-Based Intelligent Information and Engineering Systems*. 2003. Springer.

- [26] Yerazunis, W.S., et al. *A unified model of spam filtration. in Proceedings of the MIT Spam Conference, Cambridge, MA, USA. 2005.*
- [27] Subramaniam, T., H.A. Jalab, and A.Y. Taqa, *Overview of textual anti-spam filtering techniques.*

Survey on Query Processing & Optimization Techniques in WSN

Vandana Jindal¹, A.K.Verma², Seema Bawa²
Department of Computer Science and Engg.
^{1,2}Thapar University, Patiala, India.

Abstract— A WSN may be considered as a distributed database because of the presence of data in physically dispersed nodes constituting it. Data is extracted by various applications to serve the information needs. A number of techniques are being used or being introduced to extract data. Data extraction through queries is the most popular approach due to its ease of use. To combat the various limitations of limited power, bandwidth, node failure rate researchers are devising variants of querying interfaces. Main thrust is to achieve energy efficiency.

Keywords- Query processing; Query optimization; WSN

I. INTRODUCTION

Advances in fabrication and computing technologies have made it possible to produce miniature devices with sufficient computing power at affordable costs. One such category of devices is sensor nodes. Applications of these nodes have invaded every walk of life. These devices are producing a lot of data as a result of sensing physical environment continuously for which these nodes are deployed in large geographical area. These nodes can operate without wires therefore their deployment is economical. Millions of bits of data are being generated by these devices. Various database management systems have been developed to manage this ever growing data so as to facilitate information extraction. For reliable and economical information extraction a number of extraction processes have been developed. These processes/techniques from sensor networks may be categorized into three broad categories [1-3]: *agent-based*, *query-based* and *macro-programming based*.

Agent based approach: Agent is autonomous software that works independently in achieving any designated task without user's intervention. The agent based systems may have a group of agents, which team up for executing a particular task for information extraction. The agents are mobile, self replicating and capable of handling the unpredictable environmental changes [4, 5] which is a feature of WSN in many applications. The distributed databases of WSN pose a challenging task in designing the mobile agents as in WSN the resource constraints and unforeseeable weather conditions are to be taken care of. Moreover it is not an easy task to test and debug agent based system.

Macro programming based approach: The second approach is to develop macro program for WSN. In this the programmer is free from the in depth study of the system's resources,

topology etc. On the contrary the programmer is required to possess sufficient amount of knowledge and experience for developing a macro program. Although macro programming is supposed to save the programmer from the programming at the node level, however certain macro programming based systems cannot fully abstract the details at the node level. In such cases node level knowledge becomes necessary. Learning of macro programming is time consuming.

Query based approach: This is one of the widely accepted approaches for data extraction. It is based on querying the database for information retrieval. The reason for its popularity is its user friendly interface and its capability to display pertinent details to the user. Despite comfort various obstacles are associated with it also. The queries that can be issued for the information extraction are restricted to a limited extent only while displaying the sensed data and performing various aggregate computations like minimum, maximum etc. on this data. The query languages face difficulty in representing characteristics that involve both space and time, which is a key characteristic of the data sensed in the sensor network.

All the three approaches are well suited for diverse WSN applications. Undoubtedly, agent based approach and macro programming approach have an upper hand in terms of flexibility but implementing them in WSNs is not an easy task in comparison to query based approach as the user feels a great degree of comfort while working with queries. Therefore because of its popularity we shall discuss query based approaches in coming sections.

Through queries a user can get timely and reliable information economically from very large database systems running in diversified environments. Query instructs a DBMS to retrieve or update data. Complete processing of a query generally involves three steps: Parsing & translation followed by Optimization and finally Evaluation. The first step involves conversion of query into a form understandable by the query processing engine. In the next stage the query processor converts the internal data structure into equivalent but more efficient representations. This internal representation by query processor may be done on the basis of mathematical or cost models, heuristics, semantics or selection algorithms etc. Choosing these and applying them for an efficient result is the work of Query Optimization Engine, which develops some plans to be evaluated in the final phase. Finally, the evaluation

phase selects the best plan out of the various plans generated by the optimization engine keeping in view the application specific metrics such as latency, energy efficiency, security etc.

Till early 80s query processing techniques were mostly available for wired systems only. Researchers wanted to broaden the applicability of these techniques to wireless networks also, so that the use of wireless networks could be made popular. At that time wireless network applications were very few as data retrieval methods from these networks were not developed. Wireless Sensor Networks (WSNs) are a special case of wireless networks and have caught the fancy of many research and development scholars in recent past due to versatility of these networks. Applications of WSN are growing, however a number of limitations such as limited power, processing capabilities, available bandwidth hamper the growth of WSN applications. A lot of work is being done and there are a whole lot of research projects going on in WSN field. Main focus is on the optimum use of the limited resources of a WSN. Energy conservation is the need of the hour and a major limitation of WSN so all research endeavors have energy efficiency as one of the motives.

WSN consists of a number of sensor nodes deployed over a large geographical area. Each node in a WSN acts as a source of input from where the sensed data makes its way into the WSN for reaching the user. A sensor node may be compared to a small computer which stores information. Each node within a WSN is having sensed data and this can be considered as a mini database but *distributed* in nature making WSN a “*distributed database*”. To this distributed data, queries are to be applied to extract the desired information. Query processing techniques may vary so as to meet the quality of service and performance requirements. A number of evaluation metrics are employed to compare these techniques and best possible is chosen.

Some of the metrics used for evaluation of performance are *timeliness*, *accuracy*, *reliability* and *optimum usage of resources* etc. These metrics are not independent of each other. To achieve better score in one parameter, we may have to sacrifice some other parameter.

The organization of the paper is: Sec II gives us the motivation for undertaking the study in hand. Sec III brings out the differences between Traditional Query Processing and Query Processing in WSNs. Various Energy Efficient/ Conservation Approaches for WSNs have been discussed in Sec IV. Finally Sec V gives the Conclusion and Future scope.

II. MOTIVATION

Economic viability and long term reliability of WSN has always been an area of interest for research community. For long term viability, optimum use of limited resources is the prime consideration. Energy is a major constraint in WSN. Every endeavor must be to find ways and means which are frugal on energy consumption so as to increase the lifetime of the WSN as once energy is exhausted; node becomes dead which affects the network badly. The energy consumption involved in processing a single instruction is of the order of

nano Joules. However data transmission costs are manifold higher than data processing costs.

1Kb data transmission requires power equivalent to processing three million instructions.

Therefore to achieve maximum benefit in terms of energy consumption, it is essential that the number and content of transmissions is reduced without loss of other essentials such as data security, data fidelity and acceptable latency. So for maximum results transmission reduction is being targeted.

III. TRADITIONAL QUERY PROCESSING VS. QUERY PROCESSING IN WSN

A vast difference lies between query processing in traditional databases and in databases related to WSNs. Query processing in traditional databases is mostly unsuitable for WSN. In traditional databases, the best query plan chosen by query optimizer is the one which needs minimum number of disk accesses. However, in WSNs the query plan chosen by the optimizer is the one which has minimal estimated energy cost. In addition to this the difference is due to the inherent properties of the sensors constituting the wireless network. The node comprising a WSN is more prone to failures, has restricted memory size, uses vast amount of energy for data transmissions, data streaming etc. In contrast to the traditional query processing in DBMS, the input received by a sensor in a WSN is in the form of continuous data stream, in an unordered and unreliable form (due to various environmental factors). Therefore, in order to ensure efficient query processing in WSNs, resource management like- memory, energy, bandwidth etc. should be taken care of. Query processing techniques in sensor networks may be classified as: *In-network* or *Base station* (Fjording Architecture). These are also known as distributed processing or warehousing. Distributed processing [6] or In-network processing reduce transmission costs. Warehousing approach involves data transmission (for processing), to a place centrally located equipped with abundant energy.

Table 1: Difference between Traditional and WSN data processing

TYPE →	TRADITIONAL DATABASE	WSN DATABASE
FEATURES ↓		
PROCESSING LEVEL	Centralized	Centralized, Distributed
DATATYPE	Static	Real-time continuous data stream
AVAILABLE MEMORY	Available without any constraints	Restricted
COMPUTATIONAL ABILITIES	Unlimited	Restricted
AVAILABLE ENERGY	Unrestricted	Limited
RESPONSE EXPECTATION	Latency tolerable	Real-Time with minimum latency in majority cases

Main disadvantage associated with this approach is the vast amount of energy requirements for data transmission from

node to the centrally located area. Moreover, even when information is to be extracted from a small portion of the data, the warehousing approach follows the order of transmitting the whole data to the central location for processing and analysis. Main advantage is that there is centralized control which saves retransmission costs.

IV. ENERGY EFFICIENT/ CONSERVATION APPROACHES FOR WSN

Recent use of WSN in more and more applications has turned conserving energy in WSN a crucial issue. Various approaches keeping in view the priority metrics (defined above) have been devised. These approaches may be divided into three categories namely *mobility based*, *database optimization* and *duty cycling*.

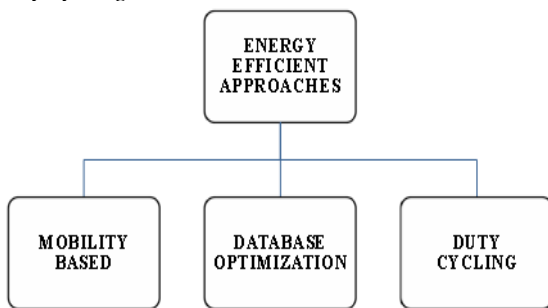


Figure 1: Various Energy efficient approaches in a WSN

A. Mobility based

The data sink is made to travel to node in a network for data collection reducing the energy consumption. The mobility based approach used for data collection is divided into two categories i.e. *i) using a single mobile sink* and *ii) using multiple mobile agents*.

In single agent approach the data packets are collected by the sink itself resulting in an efficient approach. However, the failure of mobile node leads to data loss. To overcome this problem, multiple mobile agents (sinks) are used for data collection. The mobile sinks may collect the data from the nodes by moving in a random, predictable [7] and controlled mobility fashion [8]. In this way risk of data loss in case of agent failure is eliminated.

B. Duty Cycling

In this mode, sleep and wake cycle called *duty cycle* of a node is adjusted according to the application thereby reducing wastage of energy in a node when it is idle. Sensors consume a large amount of energy in idle mode as compared to transmission mode. Therefore, the nodes which are used for sensing, reception and transmission of data are switched off when idle. Only downside of this approach is that a node may fail to detect some event when it is sleep. Moreover, switching

off of radio signals intermittently may lead to connectivity problems. Hence a tradeoff is to be maintained. By operating at a low duty cycle i.e. cycle of operation of a node which operates intermittently helps in energy conservation. It is most appropriate in conditions where sensors usually remain idle. In some conditions nodes are put to sleep (power-saving) mode for conserving energy and increasing the network lifetime.

Thus a trade-off is established between the sensing and data transmission in an intermittent manner in WSN, as nodes go into sleep and wake mode. The intermittent condition of the node sometimes fails to detect an event. Also switching off the radio signals may lead to connectivity problem between the nodes. As a result the data is unable to find the path for its transmission. Both the cases lead to latency. Hence a tradeoff between the energy conservation and performance is noticed.

C. Database Optimization

Optimization of database consists of: *data acquisition* and *data processing*.

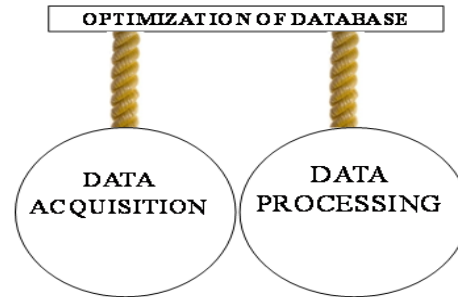


Figure 2: Various Database Optimization approaches in a WSN

• Data Acquisition

Data acquisition is the process of measuring the real-world physical conditions such as temp, light, sound etc. and converts these into digital numeric values which can be operated upon with the help of computer. Physical condition that is to be measured is initially sampled with the help of sensors. Measured signals are analog in nature. These signals are to be converted into digital form so as to get operated by the microcontroller. Elements of data acquisition system are: transducers, signal conditioners, Analog-to-Digital Convertors (ADC). Data acquisition may be summed as acquisition of signals from the environment, subjecting them to digitization and finally saving as data.

Traditional Data acquisition approaches can be categorized into: *Data logging* and *Decentralized data aggregation*. In the first case the data is acquired at various nodes and then each node transmits the data to the base station. It is a time consuming approach but limited bandwidth is used efficiently. In the second case according to Rice et al. [9] the acquired data is processed at various nodes and aggregated before its transmission to gateway node. Processing of data at nodes level leads to decrease in size of the data to be transmitted [10] thereby reducing energy consumption. According to C. Alippi et al. [11] energy efficient data acquisition can be achieved through techniques like *duty cycling* and *adaptive sensing*. In

Duty cycling sleep and wake cycle is adjusted. Adaptive sensing/ data acquisition can be done with the help of any one of the below mentioned techniques i.e. *hierarchical sensing*, *adaptive sampling* and *model-driven sampling*.

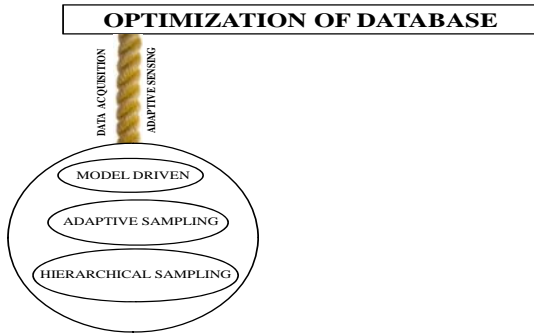


Figure 3: Various Adaptive Sensing/ Data Acquisition approaches in a WSN

Hierarchical Sampling: In this approach the sensed data moves through a path from energy rich nodes (with low energy consumption) to a nodes possessing lesser amount of energy lying in close proximity to the base station. Low energy consuming nodes are given priority in hierarchy.

Adaptive Sampling: It is based on the relationship existing between the sensed data and the energy possessed by the node. Temporal correlation exists when there is not much change in the sensed data spanning over a period of time. Spatial correlation exists when the sensors lying in close proximity sense the data with no distinction/ dissimilarity. Hybrid of both temporal and spatial correlation may be used for getting the samples, keeping in view the energy left within a node.

Model driven: In this approach a model is constructed with a set of sensed data, used for data prediction on the basis of model. The approach is energy efficient as the data sensing may be avoided (as data is predicted). Regular model updating is necessary to comply with the changing physical conditions of the area under study to maintain reasonable authenticity.

- **Data Processing**

It involves:

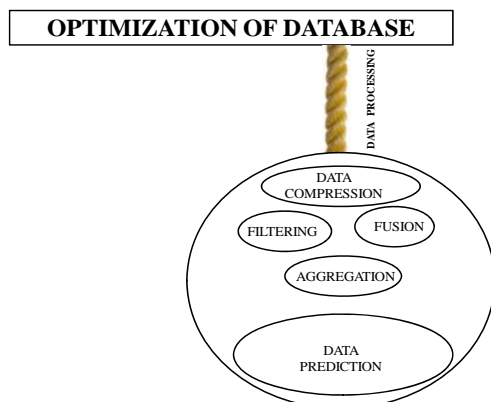


Figure 4: Various Energy Efficient Data Processing approaches in a WSN

Data compression: One of the measures adopted to optimize usage of limited resources is data compression. Data compression leads to reduction in size of the data to be transmitted leading to less bandwidth requirement for this reduced data. Amongst the three operations performed by the node in a WSN- sensing, processing and transmission, approximately 80% of the power is used in transmission process. Power consumption reduces with the data size via compression. Power is required for executing the compression algorithm. However, there is a net power gain as the cost of data compression is less than the cost of data transmission. Compression algorithms considered for the sensed data in a dense sensor network follow a *distributed approach* where as in sparse sensor network *local approach* is implemented. The advantages of using compression technique are that power optimization leads to increase in WSN's performance; reduction in cost, space & data transmission time; and finally quality of service is good.

Filtering: Besides acquisition of physical data continuously, node may be afflicted with false data injection from rogue nodes. This data injection is a major threat to network security and energy resources. Filtering technique "Bandwidth Efficient Cooperative Authentication" (BECAN) [12] is used for early detection and filtering of maximum possible false data. Source authentication to identify attacker nodes injecting false data is also employed. These techniques have high computational and communicational overheads of their own which is a drain on energy. Schemes with low authentication overhead are required and tradeoff between energy depletion due to overheads and QoS required is to be decided by the user.

Data Fusion: WSNs are deployed to monitor and measure physical environment conditions. Sometimes strong variations in these conditions affect the measurement of sensor itself resulting in imprecise or unreliable data acquisition. Data fusion techniques are employed to overcome such problems. In this data from multi sources is combined to draw out inferences which have chances to give more accurate data efficiently as compared to data given by single source. Data fusion can be applied on centralized or distributed basis. In WSN distributed fusion means fusion of data of a node and its neighbors. Data fusion is helpful in overcoming effects of sensor failure, technological limitations and spatial and temporal coverage problems through cooperation, redundancy and complementarity. Sensor nodes deployed in a network are able to cover a partial view of network. Fusion of data of nodes cooperating with each other results in complete view of the network. Redundancy helps in mitigating the effect of sensor failure and complementarity is used to make different sensors observe different parameters and fusion is used to draw out inferences which may not have been possible with single measurement.

Researchers [13, 14] define data fusion as "multilevel, multifaceted process handling the automatic detection, association, correlation, estimation, and combination of data and information from several sources".

Fusing data from multiple sources leads to data reliability and decreases the probability of errors. It provides better understandability of the WSN application under study enabling optimum execution of the response. There is confusion between 'Data fusion' and 'Data Aggregation'. No doubt there are similarities between the two but the protocols designed for them differ in terms of the number of nodes deployed (density) and the frequency with which the queries are injected. Data fusion is applied on a WSN covering a large area using compressive functions where as data aggregation is applied in a WSN covering a small area using functions like count, sum, average etc. Data fusion is implemented at regular intervals on continuous data stream; otherwise it may result into data explosion. Various models based on- input and output obtained [13], in context to software engineering [15], random sets [16] have been proposed for data fusion. Range of techniques available and their limitations make Data fusion a tough job to handle.

Data prediction: Prediction based data aggregation can be very helpful in WSN as environmental data sensed periodically has a great temporal redundancy. Prediction based approaches exploit temporal correlation of the sensed data and prepare model for data prediction. Due to changing environment model need to be updated regularly.

Data aggregation: Data aggregation aims at increasing the lifetime of the network by reducing data transmissions which are redundant. This technique aggregates the similar data sensed by various sensor nodes passing through a particular node before reaching the base station. The data may be aggregated with the help of various aggregation schemes like Low Energy Adaptive Clustering Hierarchy (LEACH) [17], Tiny Aggregation (TAG) [18] etc. The aggregation may be performed either by i) *Reducing the data size* or ii) *Without data size reduction* that is to be transmitted. The former method involves combining and compressing the data sensed at a particular node which receives the data from other neighboring nodes before allowing them to make their way to the base station. In the second method, the data that is received from other nodes is merged at a particular node which reduces communication overheads. No processing takes place on this merged data which is then forwarded to the base station.

Data aggregation can also be categorized on the basis of: i) *address* and ii) *data*. In the address based routing scheme [19] the query is sent to the particular address and this specified addressed node within the query transmits the result to the base station. In contrast to the address based routing, in data centric routing, the query is broadcast to all the nodes within the WSN which satisfy the given condition as mentioned in the injected query. All the nodes which heed to a similar condition combine their data and aggregated data makes its way to the base station.

Data aggregation techniques may be classified into i) *chain-based* ii) *tree-based* and iii) *grid-based aggregation*.

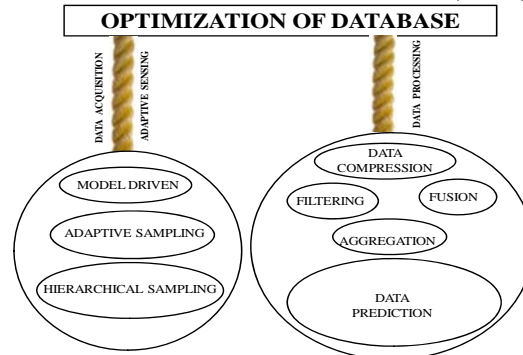


Figure 5: Various Energy Efficient Database Optimization approaches in a WSN at a glance

V. CONCLUSION AND FUTURE SCOPE

In view of the above discussions it is concluded that though there is a plethora of information extraction approaches, from WSN, each having its own pros and cons. Query based approach is the most popular because of its ease of use and its ability to serve most of the information needs from WSN. There are a number of variants of the approaches which have been developed for specific applications. To combat the inherent constraints of limited energy and bandwidth, data optimization and transmission optimization are the main areas of research. Data optimization processes and various techniques in those processes have been discussed. These processes can be used by the user according to requirement of application and resources available. Economical considerations, technological capabilities of nodes etc. play a significant role in selection of one or number of techniques of optimization of data. Future may belong to other advanced techniques such as macro programming as more and more expertise and statistical models become available.

REFERENCES:

- [1] E. Gaura, and T. Daniel, 'Information extraction from large-scale WSNs: approaches and research issues: approaches and research issues: part I: overview and agent based approaches'. *Sensors & Transducers*, volume 94 (7): 15-33, 2008.
- [2] T. Daniel, and E. Gaura, 'Information extraction from large-scale WSNs: approaches and research issues: approaches and research issues: part II: query-based and macro programming approaches'. *Sensors & Transducers*, volume 94 (7): 34-56, 2008.
- [3] T. Daniel, and E. Gaura, 'Information extraction from large-scale WSNs: approaches and research issues: approaches and research issues: part III: towards a hybrid approach'. *Sensors & Transducers*, volume 94 (7): 57-82, 2008.
- [4] H. Qi, Xiaoling Wang, and K. Chakrabarty, 'Multisensor data fusion in distributed sensor networks using mobile agents', In 5th International Conference on Information Fusion, Annapolis, MD., 2001.
- [5] C. L. Fok, G. C. Roman, and C. Lu, 'Mobile agent middleware for sensor networks: an application case study', In Proceedings of Fourth International Symposium on Information Processing in Sensor Networks (IEEE Cat. No. 05EX1086), Los Angeles, CA, USA, pp. 382-387, 2005.
- [6] P. Bonnet, J. Gehrke, P. Seshadri, 'Querying the physical world', *IEEE Personal Communications*, 7, 5, pp. 10-15, 2000.
- [7] A. Chakrabarti, A. Sabharwal, and B. Aazhang, 'Using Predictable Observer Mobility for Power Efficient Design of Sensor Networks', 2002.
- [8] I. Chatzigiannakis, A. Kinalis, S. Nikolettseas, 'Efficient data

propagation strategies in wireless sensor networks using a single mobile sink', Elsevier Computer Communication, 2008.

- [9] J. A. Rice, K. A. Mechitov, S. H. Sim, B. F. Spencer, and G. A. Agha, 'Enabling frame-work for structural health monitoring using smart sensors', Structural Control and Health Monitoring. doi:10.1002/stc.386, 2010.
- [10] J. P. Lynch, A. Sundararajan, K. H. Law, A. S. Kiremi djian, and E. Carryer, 'Embedding damage detection algorithms in a wireless sensing unit for operational power efficiency', Smart Materials and Structures, 13, no. 4, 800-810. doi:10.1088/0964-1726/13/4/018,2004.
- [11] C. Alippi, G. Anastasi, M. D. Francesco, M. Roveri, 'Energy management in wireless sensor networks with energy-hungry sensors', Instrumentation & Measurement Magazine, IEEE 12 (2), 16-23, Apr 2009.
- [12] R. Lu, X. Lin, H. Zhu, X. Liang, 'BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks', Parallel and Distributed Syst, Volume:23 Issue:1.
- [13] F. F.E. White, 'Data Fusion Lexicon', Joint Directors of Laboratories, Technical Panel for C3, Data Fusion Sub-Panel, Naval Ocean Systems Centre, San Diego, 1991.
- [14] L.A. Klein, 'Sensor and Data Fusion Concepts and Applications', second ed., Society of Photo-optical Instrumentation Engineers (SPIE), Bellingham, WA, 1999.
- [15] B.V. Dasarathy, 'Decision Fusion', IEEE Computer Society Press, Los Alamitos, CA, 1994.
- [16] I.R. Goodman, R.P.S. Mahler, H.T. Nguyen, 'Mathematics of Data Fusion', Kluwer Academic Publishers, Norwell, MA, 1997.
- [17] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, 'Energy-Efficient Communication Protocols for Wireless Microsensor Networks', Proceedings of the 33rd Hawaiian International Conference on Systems Science (HICSS), January 2000.
- [18] S. Madden, M.J. Franklin, J.M. Hellerstein, and Wei Hong, 'TAG: aTiny Aggregation Service for Ad-Hoc Sensor Networks', Appearing in 5th Annual Symposium on Operating Systems Design and Implementation

(OSDI). December, 2002.

- [19] K.Sohrabi, J.Gao, Y.Ailawadhi and G.J.Pottie, 'Protocols organization of Wireless Sensor Network', in Proceedings of IEEE Personal Communications, 7(5), 16-27, Oct. 2000.

AUTHORS PROFILE

Vandana Jindal is currently working as an Assistant Professor in the department of Computer Science at D.A.V College, Bathinda. She holds degrees of B.Tech, MCA, M.Phil. Since January 2009, she has been with the Thapar University, Patiala in Punjab as a Ph.D. student. Her research interests include database management systems, wireless sensor networks. She is a member of IEEE and IEI.

A. K. Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001 respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engineering College, Gorakhpur from 1991 to 1996. His research interests include wireless networks, routing algorithms and securing ad hoc networks.

Seema Bawa holds M.Tech (Computer Science) degree from IIT Kharagpur and Ph.D. from Thapar Institute of Engineering & Technology, Patiala. She is currently Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). Her areas of interest include Parallel and distributed computing, Grid computing, VLSI Testing and network management. Prof. Bawa is member of IEEE, ACM, Computer society of India and VLSI Society of India.

A SECURITY LEVEL STUDY IN CLOUD COMPUTING

Muzammil Nawaz
Computer Science
UET
Taxila, Pakistan

Rashid Amin
Computer Science
UET
Taxila, Pakistan

Fahad Ubaid
Computer Science
UET
Taxila, Pakistan

ABSTRACT— The cloud computing network is based upon the shared resources by its service providers these services are like online storage facility, online processing and calculations in specific way and other services. These services are charged by the providers. The cloud service is no doubt a much facilitating service but there are many security issues involved with the same. Any user shares his data on cloud for processing and for other purposes and also connects with the cloud by maintaining a network with his own device. So these factors may cause security issues while using the cloud services. There is also very large verity of study done on the security issue related to cloud computing. This study is also for the same issue related to cloud network and their possible solutions, as well as related ideas for cloud providers and researchers.

Keywords: cloud computing, security challenges, security, cloud services

I. INTRODUCTION

The term cloud is basically enveloped from the concept of networked computers and these computers are interconnected for some specific purposes. This cloud of networked computers is a group of service providers and the users of these services. In this infrastructure the providers offer the clients to facilitate them in such ways like offering Software as a service, platform as a service and infrastructure as a service. Users connect on the cloud to avail their desired service which is charged by the provider or some time some services are offered as free service also which may be advertising further charged services in their free service [1] [2]. This whole infrastructure may reduce capital and time saving for users to approach and to be used [4]. In the discussed scenario these services are publicly offered but there are non availability of there security standard. In this paper, some standards have been proposed to reduce the security problems in the clouds.

1.1 Services of Clouds

- **Services On demand:** the capability of availing cloud services when needed by the user. By signing-in to avail the service without delays.
- **The Broad Access to network:** This is the Capability of accessing the cloud services by the mean of platforms which are installed on different devices such as computers, mobile phones, tablets etc.

- **Pooling of Resource:** Because there are many customers available at a time on the cloud so Resources are well pooled among the customers.
- **Rapidly elasticity:** The capability of managing increased demand on the cloud and also scale that demand.
- **Measured Service:** The capability of invoicing on metered basis and in time sending to the users.

Here is the diagram given below showing the Stack of Cloud Computing, It demonstrates three different categories inside Cloud Computing [2][3]:

a) Software as a Service (SaaS)

b) Platform as a Service (PaaS)

c) Infrastructure as a Service (IaaS)

In SaaS Different applications offered as a service on the cloud for the use of end-users, PaaS is a specific platform like a suite of services and tools, offered to the users as service [8]. IaaS is a specific infrastructure concerned with hardware and software which is the combination of its main stack such as operating systems , networks, servers, storage etc [5][8].

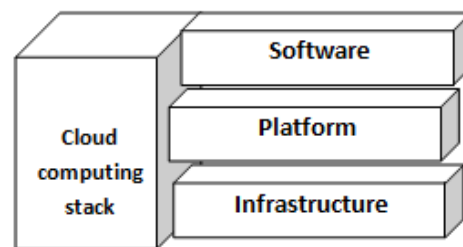


Fig 1. Stack of Cloud Computing

1.2 Characteristics of PaaS

- To provide a platform for further development and testing like IDE.
- Different interfaces for different styles of working and processing for each user separately.
- Sharing of same like resources and databases interconnectivity among the users [8].

1.3 Characteristics of IaaS

- The well distribution of resources as service

- The scalability of utilized and available resources dynamically.
- Automation of pricing for different resources used by the users [5][8].

1.4 Characteristics of SaaS

- Easy way of availing software on the websites and utilizing the offered software and applications on cloud like online processing.
- All updates related to software are time to time made only on cloud and no need of updating by each user.
- Modules and pieces of software like APIs and capability of integration for users need [6][7][8].

II. DIFFERENT TYPES OF CLOUD

2.1 General Clouds

These clouds are used for utilization of services by common people available on the cloud. These clouds are non-member based for the internet users and approachable any time without any specific registration or login. Such as a simple website offering to convert a video file format by uploading a video file and getting back a converted file into a desired format or online image processing, gaming and offering of free apps downloading etc.

2.2 Domain-Specific Clouds

This type covers a specific group of people or organizations according to the requirements of resources and services. Just like a group of researchers are kept into a specific domain or a virtual network to access digital libraries offered by cloud or the group of such related circle like medical, engineering etc.

2.3 Mixed Clouds

These clouds consist of all characteristics of all available previous clouds and capable of sharing data, resources etc as per requirements. The clouds involved in this category cover a multi range of services by offering a variety of mixed services to its users.

2.4 Personal Clouds

This type of cloud is for a personal utilization of an organization. The services offered by personal clouds are related to the requirements of organization and utilized by its members to fulfill the necessities of organizational work.

III. DIFFERENT TYPES OF SECURITY THREATS ON DIFFERENT CLOUDS

3.1 Personal Clouds

These clouds can be utilized for an organization like official and enterprise services, sharing of resources related to the organization and devices or set of devices like an infrastructure. Also for facilitating emailing and server based activities. This cloud will be available with its services within the organization so the risk factor will be reduced. The ERP software is the example of personal cloud. The applications are also distributed on specific servers so that related users can

approach related applications so the attacking factor from any other source will be reduced. The data used to avail a service will also on its related server of application and the security for the data will be increased [9][10].

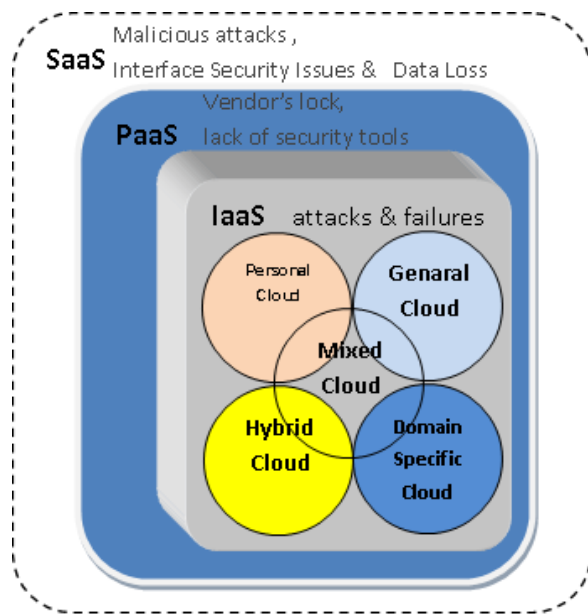


Fig 2. Classification of Clouds

3.2 General Clouds

A general cloud where a service provider makes the resources like applications and storage is offered to the public over the internet. The main advantages of using general cloud services are:

- Non expensive setup due to the hardware and resources are provided by service provider
- Resources are utilized accordingly as per demand so economically suitable for general public

Because the infrastructures and services are shared in general cloud so there may the factor of security risk. The following are the security challenges which are yet to be solved and which may give way for attackers and hackers for interruption.

- The server on which the service is running for users
- The placement of easily hack able codes and programs on the server.
- Attacks on servers.
- DoS Attacks

3.3 Domain Specific Clouds

These clouds are utilized among the groups of specific users. Following are the Security Issues in Domain Specific clouds:

- Auditing and Compliance.
- Intrusion Detection (IDS) and Firewall features.
- Access control.

- Anti Virus/Anti Malware protection.

3.4 Hybrid Clouds

The hybrid cloud is combination of private (at least one) and general (at least one) cloud. In this type of cloud computing environment an organization computes resources internally as well as externally [9][10]. Following are the risks for these clouds:

- Multiple cloud availability risk.
- Ongoing compliance concerns
- Access control and identifications.
- Data transferring

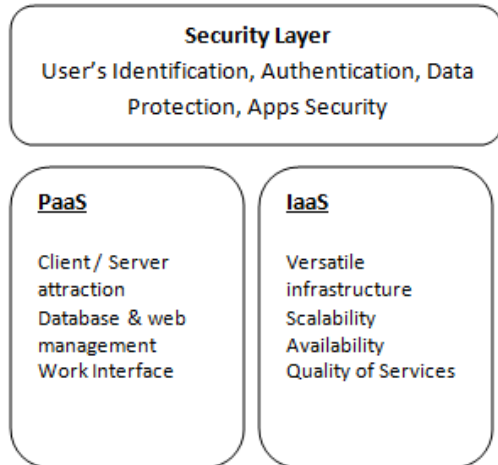


Fig 3. Security Issues in Clouds

	Services by Clouds		
	IaaS	SaaS	PaaS
Security Issues	Attacks and Failures	Malicious Attacks, Data Loss, Interface Security IssuesI	Vendor's lock, lack of security tools
Security Measures	Resorce distribution, dynamic scability, price automation	Automatic updation of software, integrated modules for users	Dynamic Interfaces, Sharing of resource Intelligent ly among users.

Table 1: of services IaaS, PaaS and SaaS

IV. CONCLUSION

In this paper various clouds are discussed regarding their security issues and possible counter measures for these issues. The discussed clouds are usable for their users separately at its own level as well as with the combination of some other cloud with it. So the security issues are also changing their shape of specifications with the changes in cloud type and combination

of different clouds types. The comparison among the clouds and among their related security issues as well as the possible solutions for security threats. Mainly involved cloud services are highlighted for their functions and the security issues on each level for SaaS, PaaS and IaaS.

Clouds	Security Issues	Security measures
Personal	Data theft	Related data server
	Attacking factor	Distributed specific apps
General	DoS attack	Secure Infrastructure
	Hackers role	Authentication
Domain Specific	Auditing	Price Automation
	Access Control	User Registration
Hybrid	Multiple clouds	Security at each cloud level

Table 2: Analysis of different clouds with respect to threat

REFERENCES

- [1] Sriram, Ilango, and Ali Khajeh-Hosseini. "Research agenda in cloud technologies." arXiv preprint arXiv:1001.3259 (2010).
- [2] Srinivas, J., K. Venkata Subba Reddy, and A. MOIZ QYSER. "Cloud Computing Basics." International Journal of Advanced Research in Computer and Communication Engineering 1.5 (2012).
- [3] Bhoyar, Rahul, and Nitin Chopde. "Cloud Computing: Service models, Types, Database and ssues." (2013).
- [4] Piplode, Rajesh, and Umesh Kumar Singh. "An Overview and Study of Security Issues & Challenges in Cloud Computing." International Journal of Advanced Research in Computer Science and Software Engineering 2.9 (2012).
- [5] Yamato, Yoji. "Automatic verification technology of software patches for user virtual environments on IaaS cloud." Journal of Cloud Computing 4.1 (2015): 1-14.
- [6] Kumar, KV K. Mahesh. "SOFTWARE AS A SERVICE FOR EFFICIENT CLOUD COMPUTING." environment 7: 10.
- [7] Rai, Rashmi, G. Sahoo, and S. Mehruz. "Securing software as a service model of cloud computing: Issues and solutions." arXiv preprint arXiv:1309.2426 (2013).
- [8] Prasanth, Anupama, et al. "Cloud Computing: A Survey of Associated Services." Book Chapter of Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications-An Open-Access eBook published by HCTL Open (2015).
- [9] Nazir, Mohsin, et al. "Cloud Computing: An Overview." Book Chapter of Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications-An Open-Access eBook published by HCTL Open (2015).
- [10] Gupta, Abhijit, and Subarna Shakya. "Information System Audit: Cloud Computing Security and Challenges." (2015).

OPTIMIZATION OF SVM PARAMETERS BASED ON MOPSO ALGORITHM

Samira Shahinfar

Abstract— Parameters selection of support vector machine is a very important problem, which has high influence on the performance of support vector machine. This paper presents a Multi-Objective Particle Swarm Optimization Algorithm (MOPSO) approach to optimize the kernel parameters. In this paper, a MOPSO is designed with two conflicting objectives to be optimized simultaneously. These two objectives are based on the error rate and a ratio of number of support vectors to the number of instances of the dataset under evaluation. To evaluate the performance of the proposed method, experiments were executed on the datasets from LibSVM (library for SVM) and the results obtained were compared with NSGAII algorithm for parameters searching. The results obtained show that the proposed approach has less error rates and vector count across some of the datasets as compared to NSGAII algorithm

Keywords: Support Vector Machine; Multi-Objective Particle Swarm Optimization; Multi-Objective Genetic Algorithm; Parameter Selection.

I. INTRODUCTION

Support Vector Machine (SVM) that is proposed by Vapnik in 1990's is a new method of machine learning. It is based on Structural Risk Minimization and Vapnik Chervonenks dimensions theory of Statistical Learning Theory. In order to obtain the best generalization ability, it searches for the best compromise between complexity of model and learning ability on the basis of limited sample information [1]. SVM has some advantages such as theoretical foundation is complete, global optimization; training time is short and good generalization performance and so on and it has been a hotspot in pattern recognition area. Parameters selection is a very important problem in SVM research area and the learning ability and generalization performance depend on the parameters selection of SVM.

The analogy of PSO with evolutionary algorithms makes evident the notion that using a Pareto ranking scheme could be the straightforward way to extend the approach to handle multiobjective optimization problems. The historical record of best solutions found by a particle (i.e., an individual) could be used to store nondominated solutions generated in the past (this would be similar to the notion of elitism used in evolutionary multiobjective optimization). The use of global attraction mechanisms combined with a historical archive of previously found nondominated vectors would motivate convergence toward globally nondominated solutions. In this paper, we proposed a method for searching for the optimal parameters of

SVM based on MOPSO and this is an efficient approach for parameters selection of SVM. The paper is organized as follows. We briefly introduce the basics of SVM classification in Section 2. In Section 3 we give MOPSO algorithm. The experiment conditions are described in Section 4. The main experiments on SVM classification and experiments analysis are shown in Section 5. In Section 6 we have concluding.

II. SUPPORT VECTOR MACHINE

The basic idea of SVM learning algorithm can be summarized two steps. Firstly, the input space is transformed to a higher dimensional linear feature space by a nonlinear transform function ϕ . Then the optimal linear separating plane can be constructed in this higher dimensional feature space. The nonlinear transformation can be realized by defining proper kernel function. The classification problem can be considered as two-class problem. Given the training data vectors $D = \{(x_1, y_1), \dots, (x_i, y_i)\}$, $x_i \in R_n$ which belongs to a class labeled by $y_i \in \{-1, 1\}$, and the goal is to separate the two classes by the hyperplane (1) which is induced from available examples.

$$(w, x) + b = 0. \quad (1)$$

where w is weight vector, b is threshold.

For non-linear problems, the optimization is to minimize the classification error as well as minimizing the bound on the VC dimension to the classifier. The optimal separating hyperplane with the constraints of:

$$y_i[(w, x_i) + b] \geq 1 - \zeta_i, i = 1, \dots, l. \quad (2)$$

minimizes the function

$$\varphi(\omega, \zeta) = \frac{1}{2} \|\omega\|^2 + c \left(\sum_{i=1}^l \zeta_i \right). \quad (3)$$

where $\zeta = (\zeta_1, \dots, \zeta_l)$, ζ_i is a measure of the misclassification errors, C is a constant which controls the tradeoff between the complexity of the decision function and the number of training examples misclassified.

The optimization problem (3) under the constraints of Equation (2) can be transformed to its dual problem.

$$\text{Max: } W(\alpha) = \sum_{i=1}^n \alpha_i - \frac{1}{2} \sum_{i=1}^l \sum_{j=1}^l y_i y_j \alpha_i \alpha_j K(x_i, x_j). \quad (4)$$

with constraints (5)(6)

$$\text{ST: } \sum_{i=1}^n y_i \alpha_i = 0. \quad (5)$$

$$0 \leq \alpha_i \leq C, i = 1, \dots, l. \quad (6)$$

where α_i is Lagrange multiplier.

SVM is a linear maximal margin classifier in a high-dimensional feature space where data are mapped through a non-linear function $\phi(x_1) \cdot \phi(x_2) = K(x_1, x_2)$.

In order to get the optimal hyperplane in feature space, kernel function should be used. Usually, Radial Basis Function(RBF) is used as the kernel function

A. Selection of the Kernel Function

The most common kernel functions available include linear, Radial Basis Function (RBF), sigmoid, and polynomial kernels which are given in eq. (7), (8), (9), (10) respectively [14]. In order to improve classification accuracy, the parameters for these kernel functions should be appropriately set.

Linear kernel function:

$$K(x_i, x_j) = x_i * x_j \quad (7)$$

polynomial kernel function:

$$K(x_i, x_j) = (kx_i x_j + c)^d \quad (8)$$

Radial Basis Function:

$$K(x_i, x_j) = \exp\{-\gamma^* |x_i - x_j|^d\} \quad (9)$$

sigmoid kernel function:

$$K(x_i, x_j) = \tanh(kx_i x_j + c) \quad (10)$$

B. Impacts of the Parameters

The generalization ability of SVM algorithm depends on a set of parameters, including the penalty factor C, the estimated accuracy and the RBF kernel parameter [3].

- Impact of the penalty factor C: The aim of the penalty factor C is to modulate the ratio between the space credibility and the experience risk in a certain digital space, so as to attain the best generalization ability for the machine model. Different digital space requires different optimal parameter C. In certain digital space, a small value of C could lead to weak punishment for the experience error, little complexity of learning machine

yet large experience risk, or vice versa. The former is called "lesstrained", and the latter is called "over-trained". When C exceeds a certain value, the complexity of SVM achieves the maximum tolerated by the data space, and the experience risks and generalization ability would not change any more. In each digital space there exists at least one suitable C to achieve the best generalization ability.

- Impacts of the RBF kernel parameter: RBF kernel parameter reflects the distribution or scope characteristics of training sample data, which defines the width of local neighborhood. A large γ means relatively little variance.

Impacts of the estimated accuracy: The relaxation factor determines the width of the non-sensitive zone, and affects on the number of support vectors. By selecting a small value, the regression estimation becomes greatly accurate. However, in that case, the number of the support vectors and the complexity of SVM algorithm would both increase. By selecting a great value, regression estimation becomes less accurate, but the number of the support vectors could decrease and the complexity of SVM algorithm would be weakened. Similar to the relaxation factor, the estimated accuracy has the same impacts on the system.

Therefore, in the standard support vector machines, parameters C and determine the complexity of the model through different ways [2].

III. MULTI-OBJECTIVE PARTICLE SWARM OPTIMIZATION ALGORITHM MOPSO

The analogy of PSO with evolutionary algorithms makes evident the notion that using a Pareto ranking scheme could be the straightforward way to extend the approach to handle multiobjective optimization problems. The historical record of best solutions found by a particle (i.e., an individual) could be used to store nondominated solutions generated in the past (this would be similar to the notion of elitism used in evolutionary multiobjective optimization). The use of global attraction mechanisms combined with a historical archive of previously found nondominated vectors would motivate convergence toward globally nondominated solutions [4].

A. Main Algorithm

The algorithm of MOPSO is the following [4].

- 1) Initialize the population :
 - (a) FOR I=0 TO MAX /*MAX=number of particles*/
 - (b) Initialize POP[i]
- 2) Initialize the speed of each particle:
 - (a) FOR i = 0 TO MAX
 - (b) VEL[i] = 0
- 3) Evaluate each of the particles in POP[i].
- 4) Store the positions of the particles that represent nondominated vectors in the repository .
- 5) Generate hypercubes of the search space explored so far, and locate the particles using these hypercubes as coordinate system where each particle's coordinates are defined according to the values of its objective functions.

- 6) Initialize the memory of each particle (this memory serves as a guide to travel through the search space. This memory is also stored in the repository):
 - (a) FOR $i = 0$ TO MAX
 - (b) $PBEST[i] = POP[i]$
- 7) WHILE maximum number of cycles has not been reached DO
 - a) Compute the speed of each particle¹ using the following expression: where (inertia weight) takes a value of 0.4; and are random numbers in the range ; is the best position that the particle has had; 2 is a value that is taken from the repository; the index is selected in the following way: those hypercubes containing more than one particle are assigned a fitness equal to the result of dividing any number (we used in our experiments) by the number of particles that they contain. This aims to decrease the fitness of those hypercubes that contain more particles and it can be seen as a form of fitness sharing. Then, we apply roulette-wheel selection using these fitness values to select the hypercube from which we will take the corresponding particle. Once the hypercube has been selected, we select randomly a particle within such hypercube. is the current value of the particle .
 - b) Compute the new positions of the particles adding the speed produced from the previous step
 - c) Maintain the particles within the search space in case they go beyond their boundaries (avoid generating solutions that do not lie on valid search space). When a decision variable goes beyonds its boundaries, then we do two things: 1) the decision variable takes the value of its corresponding boundary (either the lower or the upper boundary) and 2) its velocity is multiplied by (1) so that it searches in the opposite direction.
 - d) Evaluate each of the particles in .
 - e) Update the contents of together with the geographical representation of the particles within the hypercubes. This update consists of inserting all the currently nondominated locations into the repository. Any dominated locations from the repository are eliminated in the process. Since the size of the repository is limited, whenever it gets full, we apply a secondary criterion for retention: those particles located in less populated areas of objective space are given priority over those lying in highly populated regions.
 - f) When the current position of the particle is better than the position contained in its memory, the particle's position is updated using The criterion to decide what position from memory should be retained is simply to apply Pareto dominance (i.e., if the current position is dominated by the position in memory, then the position in memory is kept; otherwise, the

current position replaces the one in memory; if neither of them is dominated by the other, then we select one of them randomly).

g) Increment the loop counter.

8) END WHILE

IV. SVM PARAMETERS OPTIMIZATION ALGORITHM BASED ON MOPSO

Model selection is an optimization process which requires the choice of several efficient criteria to be optimized [5] . The accuracy of classification and risk of classifier are often used to evaluate the performance of SVM. Therefore, we consider the following two objectives to be optimized simultaneously. The first one is error rate which needs to be minimized and is given by:

$$A. F(1) = \text{ErrorRate} / N_m \quad (11)$$

The risk can be estimated by VC dimension. But the VC dimension is difficult to estimate. So we have used a simple bound T for the leave-one-out error given in [1] as our second objective:

$$B. F(2) = N_{sv} / N_m \quad (12)$$

Where N_{sv} is the number of Support Vectors and N_m are the of training examples. The whole process of the MOGA approach is shown in Fig. 1 below:

Identify applicable sponsor/s here. If no sponsors, delete this text box (sponsors).

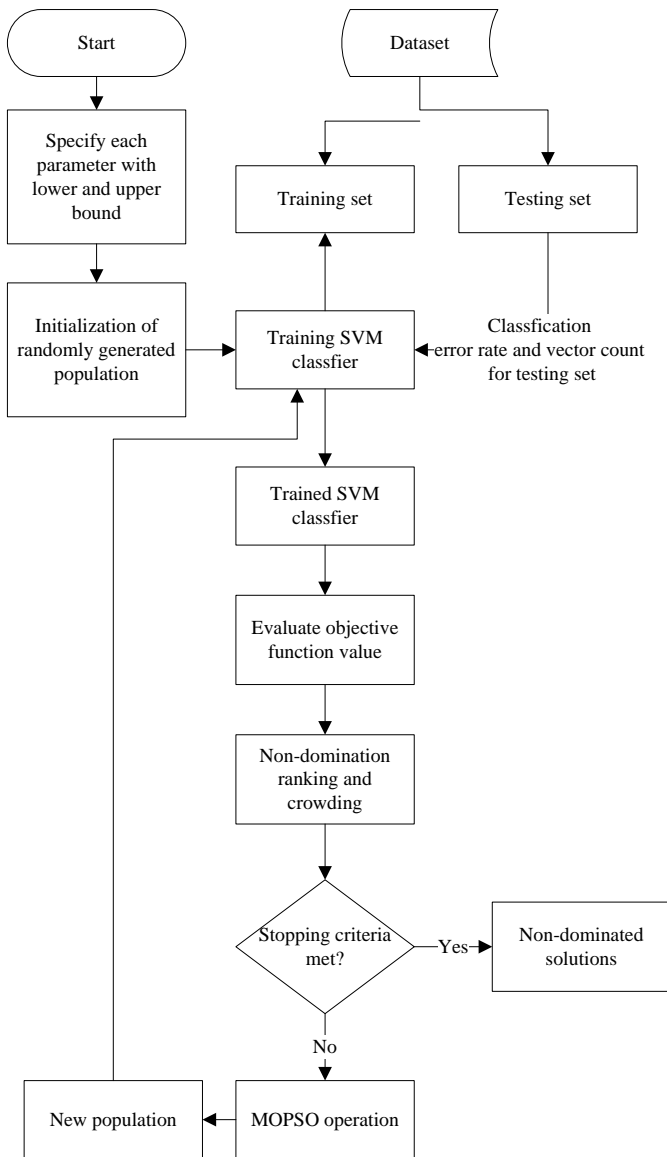


Fig. 1 The MOPSO based approach

V. EXPERIMENTAL RESULTS AND ANALYSIS

We have executed our experiments on the MATLAB 2010 using LibSvm. LibSvm is a library for support vector classification. A general use of LIBSVM involves two steps: first, a training data set is used to obtain a model and subsequently the model is validated on a test data set for predictive power. The empirical evaluation was performed on Intel Corei7 CPU running at 1.73 GHz, 4GB of RAM and windows 7 professional Operating System. The proposed MOPSO based model selection is validated on five datasets taken from LibSvm webpage [6]. Table I describes these datasets in terms of number of attributes, instances and classes.

Table I: Datasets Information

Database	Sample
Australian	690
Breast Cancer	683
Diabetes	768
Ionosphere	228
Liver Disorder	345

Table II: Parameters of MOPSO used for classification

Features	Parameters
Population size	100
Repository Size	100
Personal Learning Coefficient	-1.026
Global Learning Coefficient	-1.026
Grid Inflation	0.1
Number of Grids	10
Leader Selection Pressure	4
Repository Member Selection Pressure	2
Termination criterion	Equation(11,12)
Maximum number of generation	500

For each test database in the benchmark we picked, the following test procedures are performed:

1. Adjust the parameters of the SVM classifier with training sets in the database and test the classification performance with the testing sets in the database.
2. Adjust the parameters of the SVM classifier with one training set randomly selected from the training sets in the database and test the classification performance with all testing sets in the database as follows. In order to demonstrate the feasibility of our method, the experiments consist of following two parts corresponding to different test databases.
 - (a) The experiments are performed on MOPSO with objective function (11,12) and parameters in Table II to run experiments on different databases to validate the method respectively to select parameters for SVM classification and are stopped if the classification error rate and vector count do not change in 500 iteration runs.
 - (b) The experiments are performed on NSGA-II [7] with objective function (11,12).

Table III: Comparison of Error Rate

Database	Itr 100	Itr 200	Itr 300	Itr 400	Itr 500
Australian	1.3843	1.3899	1.3861	1.3861	1.3861
Breast Cancer	0.8366	0.7321	0.7300	0.7300	0.7300
Diabetes	1.2172	1.2167	1.2167	1.2167	0.2187
Ionosphere	0.6588	0.6667	0.6605	0.6772	0.6605
Liver Disorder	1.7125	1.3588	1.4354	1.3542	1.5426

Table IV: Comparison of Error Rate

Database	Itr 100	Itr 200	Itr 300	Itr 400	Itr 500
Australian	0.3229	0.3124	0.3120	0.3120	0.3120
Breast Cancer	0.1063	0.1050	0.1099	0.1099	0.1099
Diabetes	0.2182	0.2204	0.2204	0.2204	0.2187
Ionosphere	0.0990	0.0920	0.0942	0.0852	0.0942
Liver Disorder	0.3723	0.3458	0.3408	0.3448	0.3447

Table V: Comparison of Vector Count

Database	Itr 100	Itr 200	Itr 300	Itr 400	Itr 500
Australian	0.3145	0.3160	0.3160	0.3152	0.3076
Breast Cancer	0.1100	0.1100	0.1057	0.1057	0.1006
Diabetes	0.2241	0.2206	0.2206	0.2186	0.2186
Ionosphere	0.0978	0.0955	0.0856	0.0955	0.0830
Liver Disorder	0.3599	0.3574	0.3492	0.3509	0.3509

Table VI: Comparison of Vector Count

Database	Itr 100	Itr 200	Itr 300	Itr 400	Itr 500
Australian	1.4261	1.4058	1.4058	1.4029	1.4093
Breast Cancer	0.7701	0.7701	0.7514	0.7514	0.7338
Diabetes	1.0794	1.2117	1.2117	1.1885	1.1885
Ionosphere	0.6579	0.7351	0.6588	0.7351	0.6623
Liver Disorder	1.5391	1.4945	1.3965	1.5281	1.5281

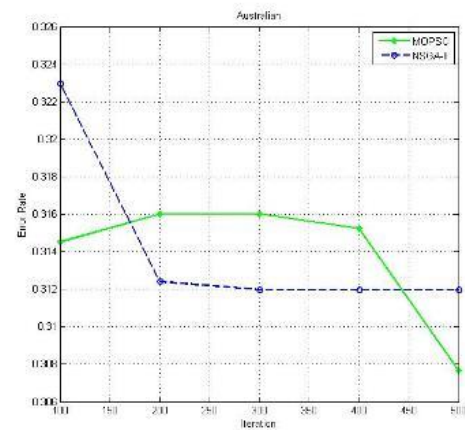


Fig. 2 Classification error rate of SVM classifier

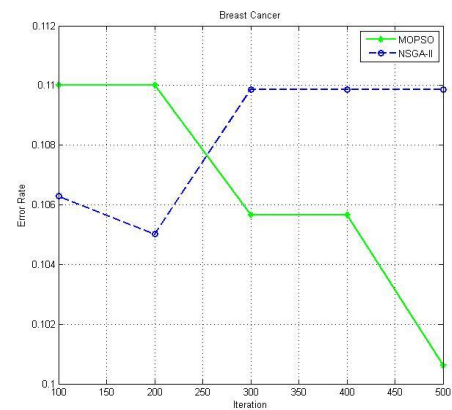


Fig. 3 Classification error rate of SVM classifier

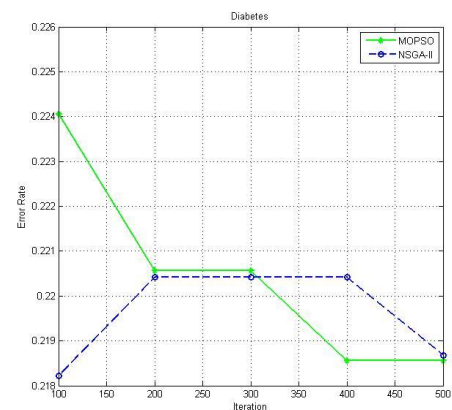


Fig. 4 Classification error rate of SVM classifier

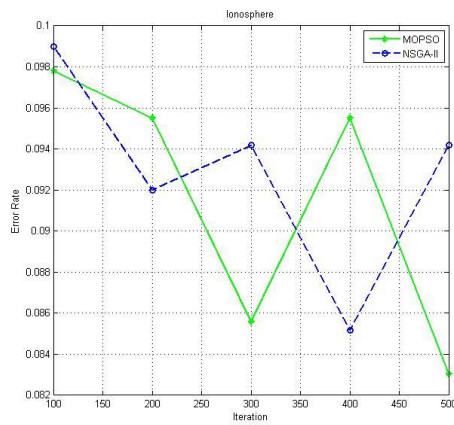


Fig. 5 Classification error rate of SVM classifier

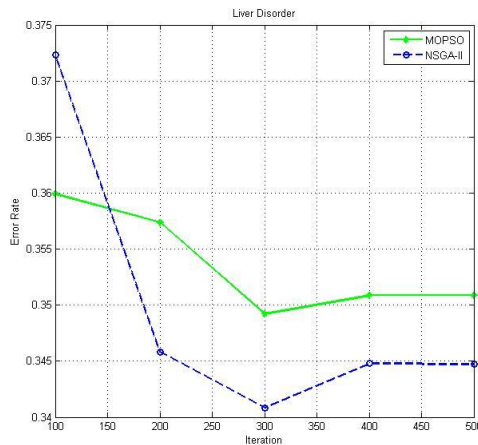


Fig. 6 Classification error rate of SVM classifier

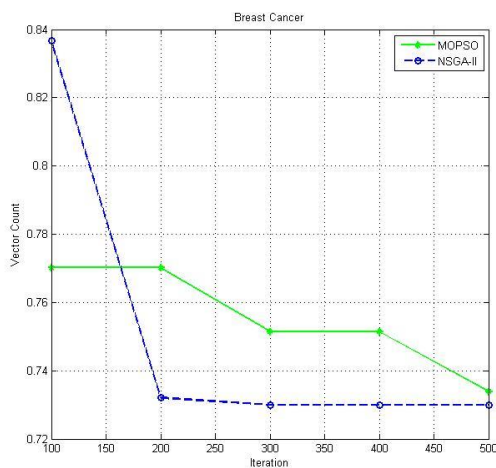


Fig. 7 Classification error rate of SVM classifier

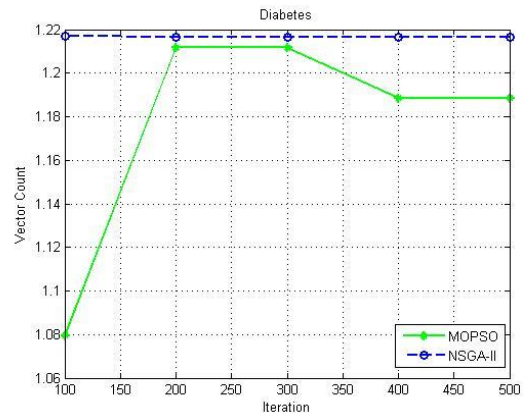


Fig. 8 Classification error rate of SVM classifier

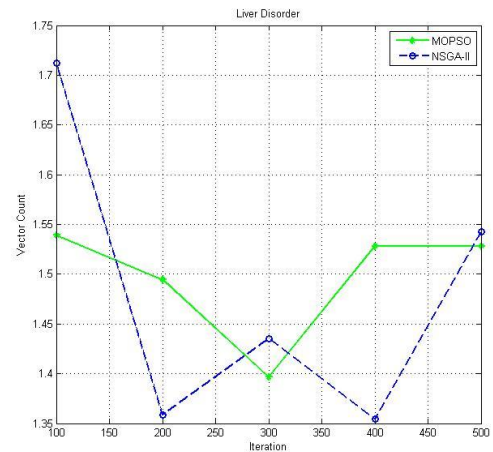


Fig. 5 Classification error rate of SVM classifier

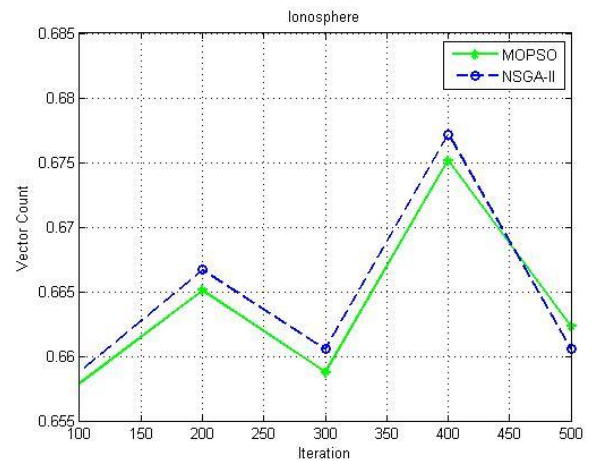


Fig. 9 Classification error rate of SVM classifier

VI. CONCLUSION

In this paper, we presented a MOPSO based approach to SVM model selection. A SVM model selection is multi-objective optimization problem, therefore, MOPSO based approach has been applied to optimize the parameters of SVM according to two objectives such as error rate and vector count. We conducted experiments to evaluate the performance of the proposed approach with five different database and the results obtained were compared with those obtained with NSGAII algorithm. The results obtained show that the proposed approach has less error rates and vector count across some of the datasets as compared to NSGAII algorithm.

REFERENCES

- [1] Zhiyu Zhu, Bing Zhang, and Weiting Liu, "A Speech Recognition Method Based on Fuzzy SVM", Computer Engineering, Vol. 32, No. 2, pp. 180-182, 2006.
- [2] S. Gao-li and D. Fang-ping. "Introduction to Model selection of SVM Regression[J]", Bulletin of Science and Technology, Vol. 22, No. 6, pp. 154-157, 2013.
- [3] O. Chapelle and V. Vapnik and O. Bousquet and S. Mukherjee. "Choosing multiple parameters for support vector", machines. Machine Learning, Vol. 46. No.1, pp.131-159, 2002.
- [4] C. Coello Coello G. Lamont D. Van Veldhuizen. "Handling Multiple Objectives With Particle Swarm Optimization", IEEE Transaction on Evolutionary Computation, Vol. 8, NO. 3, 2004.
- [5] D. Wang and W. Xiangbin. "The Optimization of SVM Parameters Based on PSO", Computer Applications, 2008, Vol. 28, No. 1, pp. 134-139.
- [6] LIBSVM - A Library for Support Vector Machines. (Available at: <http://www.csie.ntu.edu.tw/~cjlin/libsvm/>).
- [7] K. A. Saroj. "Multi-Objective Genetic Algorithm Approach to SVM Kernel Functions Parameters Selection. Computer Applications". The International Journal Of Engineering And Science (IJES), Vol. 2, No. 6, pp. 92-101, 2013.

Neural networks in the medical decision making

Manel Zribi

Faculty of Economic and Management
Sfax University
Tunisia

Younes Boujelbene

Faculty of Economic and Management
Sfax University
Tunisia

Abstract- This paper applies neural networks with an incremental algorithm as a tool to select the most relevant risk factors in the breast cancer disease. The results show that the neural approach with incremental algorithm is relevant in this research field. Using a sample of 248 Tunisian patients affected by this disease, we were able to identify the optimum combination of the factors that help reach a good predictive performance of the type of malignant and benign tumors.

Keywords-ANN, incremental algorithm, risk factor classification

I. INTRODUCTION

Cancer epidemiology is a little known in Tunisia. However, some studies have tried to ascertain this standardized impact relative to the world population by estimating that, every year, there are about 17 / 100 000 women who suffer particularly from breast cancer, which is the most common female cancer. It is the leading cause of death among women between 35 and 55 years old. The evolution of this cancer is confusing however, getting prognostic factors, as soon as the diagnosis is made, helps visualize a graduated treatment adapted to each prognostic group of patients to cope with the disease at an early stage.

For the last ten years, the use of artificial neural networks (ANNs) has evolved in many disciplines (in economics, ecology, environment, biology and medicine ...). These networks are especially applied to solve classification, prediction, categorization, optimization, pattern recognition and associative memory problems (Drew and Monson, 2000).

In the data processing framework, the ANNs, which are an approximation method of complex system due to their ability to be a universal approximator, have proven capable of extracting experimental data from successful models without having to make an assumption on the general form of these models (Thomas Pet G.Bloch, 1999).

The most widely used ANN family in the recent years, as a decision support tool, is the multilayer perceptron (PMC). This type of network has been applied in the therapeutic decisions to process data for anthropology (Benoit Blanc et al., 2001),

predict fractus (Baxt, 1995), diagnose lung (Patil et al., 1993), diabetes (Armoni, 1998), cancer (Han et al., 2001), and Alzheimer's diseases (Hamilton et al., 1997), etc.

This paper is not designed to examine in detail how the neural networks work given that many articles and books did this (Davallo and Naim, 1990; Bourret et al., 1991; Abdi, 1994; Cross et al., 1995). However, we would like to show the interest of this predictive tool through the selection of variables (Baxt, 1995; Mert, Kiliç, Bilgili, and Akan 2015; Nahato, Nehemiah, and Kannam 2015; Dheeba, Singh, and Selvi 2014; Erdem. A 2012).

II. ARTIFICIAL NEURAL NETWORKS

The ANNs are input-output models based on a character of biological neurons. The initial goal of this modeling is to rebuild the interpolating and classifying capabilities of the human brain. According to (Haykin, 1994), an ANN is a process distributed massively parallel manner, which has a natural propensity for storing experimentally knowledge and make it available for use. It resembles the brain in two points:

- knowledge is acquired through a learning process
- the weights of connections between the neurons are used for knowledge storing.

The Multilayer Perceptron (MLP)

The multilayer Perceptron (PMC) is the most used network. It is a type of feedforward network composed of successive layers and very efficient for the classification problems.

The idea consists in classify the neurons by interconnected layers. The first, which is called the input layer, is composed of a number of neurons with the task of receiving information from the outside. This information is processed and then transmitted to the neurons of the inter-layers which will in turn treat it and then send the results to a final layer called the output layer. (Fig1).

application, we use an incremental algorithm-based technique (Dunkin, N 1997) performed in 4 steps:

The first step consists in training a minimum network made up of a single neuron on its hidden layer. As soon as the learning process stabilizes, in other words, the improvement of the error compared to the previous step is inferior to a given threshold, the network stands still and a new neuron is added to the hidden layer. (Fig 2).

- The learning process starts again but only the weights of the last neuron are fixed.
- Then, the process passes onto adding neurons to the hidden layer whenever the network improvements are not significant.
- The process stops once the global network error reaches the desired threshold or when adding a new neuron does not improve the error obtained in the previous iteration.

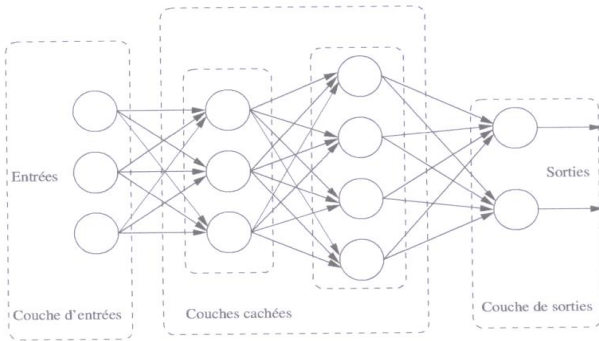


Figure 1. Multilayer Perceptron

Given the lack of theoretical rules to identify the optimal architecture of a neural network for a particular situation, several authors, such as (Mendelson 2001 Wierenga and Kluytmans 1994 and Venugopal Baets, 1994, Shepard 1990), proposed empirical rules based on a number of tests obtained by varying the number and size of the intermediate layers. Finally, it should be noted that some attempts to automatically identify the best architecture have been proposed.

III. METHODOLOGY

Our analysis is based on a sample of 248 patients suffering from breast cancer for whom the nature of the tumor (malignant or benign) is known.

The diagnosis and the care were made by a committee composed of a team from the gynecological and obstetric service at the University Hospital of Sfax, Tunisia. The period of our study extends over four years (2007-2011). A data collection sheet was prepared for each patient. The analyzed variable is the "Type of tumor", which represents the nature of the cancer (benign or malignant). Which takes the value 4 when the tumor is malignant, and 2 if it is benign. Furthermore, 17 explanatory variables of different types, epidemiological, (age, origin, marital status, contraception ...), clinical (inflammatory signs, nipple, ganglia) laboratory (mammography, metastasis,...), TNM classification, were selected and presented in the breast cancer medical card.

A. Network architecture

However, as with any neural application, the crucial point in the modeling phase is the identification of the network structure. Even if the work of (Cybenko, Funahashi 1989 and 1989) showed that one hidden layer using sigmoid type activation functions was sufficient to approximate any nonlinear function with required accuracy, nothing is known a priori about the used number of the hidden neurons.

The problem of reducing the model was initiated by (Zeigler, 1976) for whom complicity model depends on the number of elements, connections and model calculations. In our research process about the network structure that best fits our

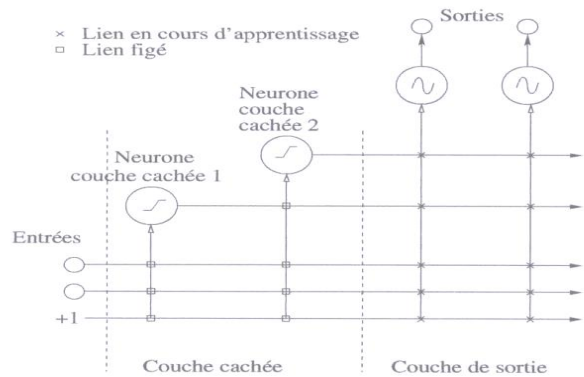


Figure 2. Incremental algorithm

This work is intended to identify the most effective learning algorithm in our study. This type of algorithm will be specified for each type of variable.

The development of such an incremental construction algorithm will help us achieve a learning back-propagation gradient type by reducing the number of neurons in the hidden layer of a feed-forward network type. (Fig 3).

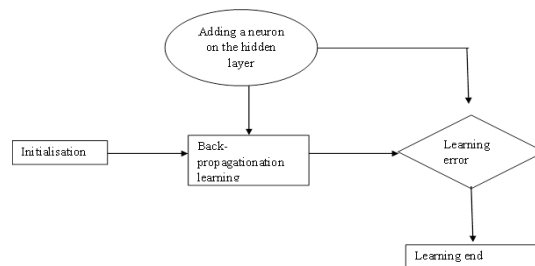


Figure 3. Learning Algorithm

The overall sample was divided into three sub samples:

- The first sub-sample, which includes 70% of the starting sample, is a learning sample.
- The second sub-sample, which is called a test sample and represents 15 % of the overall sample, is used to examine the learning sample results.
- The third sub-sample is a validation sample which represents 15% of the overall sample and is used to validate the results.

The evaluation of the network performance is carried out on the basis of:

- the minimum squared error (MSE)
- good clearance rate in the 3 sub-samples.

Generally, a network may have different activation functions for different nodes in the same or different layers (Schöneburg (1990) and Wong (1991)). However, almost all the networks use the same activation functions particularly for the nodes of the same layer. While most researchers use logistic activation functions for the hidden nodes, Klimasauskas (1991) shows that the sigmoid activation functions are more effective for the classification problems. (Table1).

Similarly, there is no consensus on which the activation function should be used for the output nodes several researchers use linear output nodes (Lapedes et Farber (1988); Weigend et al. (1992); Gorr et al. (1994); Vishwakarma (1994);Cottrell et al. (1995).

TABLE 1. Training Résultats

Number of hidden nodes	2	3	4	5	6	7
Performance to MSE (%)						
Total sample	15,20%	13,56%	11,73%	17,39%	20,24%	14,79%
Learning sample	15,73%	14,65%	10,06%	16,37%	19,06%	12,00%
Validation sample	10,99%	9,31%	11,60%	19,75%	12,11%	19,98%
Test sample	16,92%	12,68%	19,68%	19,84%	33,93%	22,75%
Good classification rate Global						
2 highly ranked	66,74%	69,26%	75,90%	56,01%	49,58%	77,66%
4 highly ranked	90,51%	91,14%	94,51%	83,80%	87,93%	83,57%
TOTAL	81,05%	82,26%	87,10%	72,58%	72,18%	81,05%

Regarding the results obtained in our application (Table 1), it can be noted that a neural network with 4 neurons on the hidden layer gives the best results. Actually, the error term in the learning sample is 10.06%, in the test sample 11.60%, and in the validation sample 19.68%, which means that the overall performance (the error measured in the whole sample) is 11.72%.

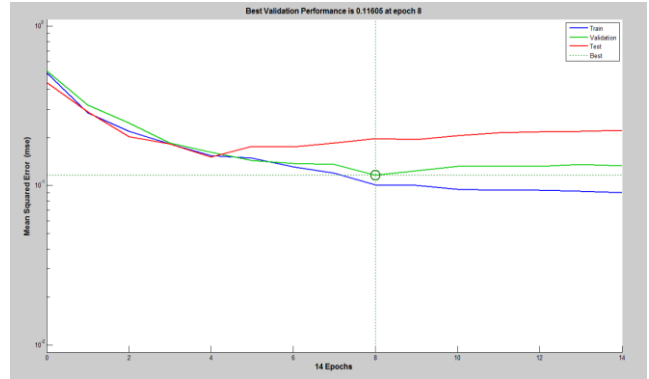


Figure 4. Performance with MSE

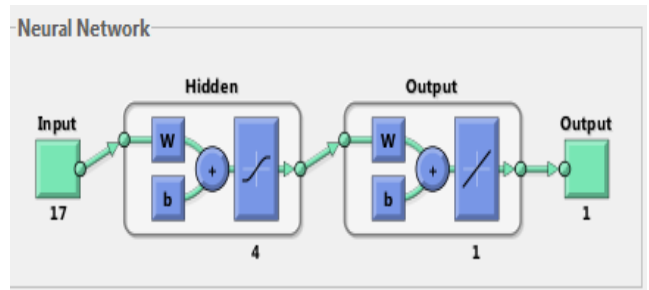


Figure 5. Optimum neural network

The chosen network (with 4 neurons on the hidden layer) helps us reach a good overall ranking rate (obtained at the level of the whole sample) of 87% of the patients having only the features of the latter (input variables).

However, it can be observed that the good ranking rate for patients who have a benign tumor (2 high ranked) differs significantly from that of patients who have a malignant tumor (4 high ranked). At the level of the whole sample, the rate of a well-ranked '4' is 94% while that of high ranked '2' is 75%.

The good results obtained in our application confirm the superiority of the neural network models compared to the probabilistic methods and classification statistics. However, compared to other empirical studies that use neural networks in the medical field, our results are slightly lower.

- Mert, Kiliç, Bilgili, and Akan (2015), they proofed that a one-dimensional features vector obtained from (ICA) causes Radial Bases Function Neural Network (RBFNN) on breast cancer classification to be more

distinguishing with the increased accuracy from 87.17% to 90.49%.

- Nahato, Nehemiah, and Kannan (2015), used a rough set indiscernibility relation method with back propagation neural network (RS-BPNN). The accuracy obtained from the proposed method was 98.6% on breast cancer dataset.
- Dheeba, Singh, and Selvi (2014), investigated a new classification approach for detection of breast abnormalities in digital mammograms using Particle Swarm Optimized Wavelet Neural Network (PSOWNN). They applied a pattern classifier. They achieved 93.671%, 92.105% and 94.167% for accuracy, specificity, and sensitivity, respectively.
- Erdem. A (2012) used an artificial neural network with a back-propagation gradient algorithm. The sample he used includes 699 WBCD (Wisconsin Breast Cancer dataset) patients and divided into two subsamples, 490 for learning and 209 for the test. The network, which has 9 input variables, 4 hidden neurons and two output neurons (malignant and benign), offers a good rating rate of 99.28.
- Marcano. A (2011) used a sample of 410 WBCD patients for learning and 273 for the test sample. The network consists of an input layer, 9 input neurons and 4 hidden neurons related to the output layer (malignant and benign tumor) by means of a sigmoidal activation function and a learning algorithm AMMLP (Artificial Metaplasticity Algorithm with multi-layer perceptron). The results provide a good ranking rate of 99.63.
- Murat.K (2009) used the same database as what was used in the previous studies (WBCD), a network of nine input variables, one hidden layer having 11 hidden neurons and an output layer with a linear function. The learning algorithm used is the gradient back-propagation to reach 95.2% of well classified patients.
- Verna (2008) used the RNA with an algorithm based on the technique of soft clustering, the learning settings called SCNN (Soft Cluster Neural Network) based on the technique of soft clustering using examples from the DDSM database (Database of Digital Mammography Screening). This technique resulted in a good ranking rate of 94%.

As a consequence, this inferiority may be caused by the small sample size compared to the various studies already carried out because the more important learning is, the better the result will be. Beyond the network's ability to recognize and properly classify the individuals presented at the input through

a battery of variables, we tried to better make use of the results so as to give other elements for a more accurate analysis. Furthermore, the undertaken learning network enables us to study the contribution of each input variable in the explanation of the studied phenomenon.

B. Risk factor classification

Determining the relevant variables is an essential step in identifying the models. The number of variables must be sufficient so that the selected model can adequately explain the studied phenomenon.

A first solution consists in studying all the possible variable combinations. It is obvious that this procedure becomes extremely heavy as soon as the number of the variables that come into operation becomes high. An optimal approach requires a tool with which we can assess the importance of each variable which helps compare different subsets, define a selection strategy for the exploration of the space of the variables combinations, and finally set a criterion for the procedure termination.

The variable selection technique adopted here consists, once the best architecture is determined, in removing an input variable each time then proceeding to learn the network and evaluate the new performance. The weaker this performance is, compared to that of the starting network, the more relevant the variable in the chosen model is. Therefore, we can classify the system input variables according to their relevance for the explanation of the phenomenon in question.

In fact, the more important the variable is, the higher the performance difference is, after the elimination of the variable and vice versa.

This technique helps us not only rank the variables, but also find the best combination among the variables presented at the system input, which reduces the complexity of the model through a non-significant loss in terms of performance. Table 2 summarizes the results of this procedure.

TABLE 2. Risk factor classification

Relevance ranking	variable eliminated	MSE obtained by removing the variable input (en%)	<u>1/ Loss of performance</u>
	Aucune	11,73%	0,00%
1	Contraceptive pill taking	21,79%	10,06%
2	Skin conditions	21,36%	9,63%
3	Breastfeeding	20,14%	8,41%
4	Metosis	17,60%	5,87%
5	State of nipple	17,41%	5,69%
6	Tumor size	16,36%	4,64%
7	Root	15,85%	4,13%
8	Age first pregnancy	15,47%	3,75%
9	Ganglion	15,03%	3,30%
10	Nodule	14,40%	2,67%
11	Menopause	14,12%	2,39%
12	Marital status	13,94%	2,21%
13	Family Previous history	13,87%	2,14%
14	Inflammatory signs	13,61%	1,89%
15	Personal history	12,81%	1,09%
16	Mammography	12,63%	0,91%
17	Age of maturity	12,32%	0,59%

According to these results, there are variables that can form a first group of great importance to the breast cancer problem. It is about the "contraceptive pill taking", 'the skin conditions' and 'breastfeeding'. The loss, in terms of performance, is 10.06%, 9.63% and 8.41%, respectively. The second group consists of 11 variables with performance losses ranging from 5.87% to 2%.

Finally, the third group consists of 3 variables which, apparently, do not have a significant explanatory power since, once one of them is deleted at the entry, the loss in the model performance does not exceed 1%.

IV. CONCLUSION

Our project is in line with the branch of the decision-making support and health economics. The desire to acquire new knowledge about the biology of breast cancer requires intelligent approaches that can be adaptable to high-dimensional data and uncertainties. This approach tested according to their relevance in the detection of the risk factors of breast cancer and their classification of patients depending on two types of tumors, benign or malignant.

Breast cancer development is often confusing. Many studies based on large series of patients identified the significant prognostic parameters for the overall survival time. These parameters will be highlighted in our study due to the importance of the early diagnosis in improving the cancer prognosis.

Knowing the prognostic factors is of a great importance because it helps measure the risk, adapt the given treatment, and especially improve the knowledge about the natural history of the disease.

Indeed, identifying breast cancer patients having a risky pattern of reactions makes it possible to give these patients specific care. Undoubtedly, this could significantly improve their quality of life. For this reason, we had better conduct our research in this context that.

REFERENCES

- [1] Drew, P., Monson, J. (2000). 'Artificial neural networks', Surgery 127:3-11.
- [2] Thomas, P. and Bloch, G. (1998). Robust ptuning for multi layer perceptrons, IMACS/IEEE,CESA'98, Nabeul-hammamet.
- [3] Baxt (1995). 'Application of artificial neural networks to clinical medecine', The Lancet 346: 1135-1138.
- [4] Patil, S., Henry, J.W., Rubenfvie, M., Stein, P. D. (1993). ,Neural network in the clinical diagnosis of acute pulmonary embolism', Chest 10:1685-1689.
- [5] Armoni, A. (1998). 'Use the networks in medical diagnosis', Medical Diagnosis Computing 15:100-104.
- [6] Han, M., Snow, P. M., Partin, A.W. (2001). 'Evaluation of artificial neural networks for the prediction of pathologic stage in prostate carcinoma', Cancer 91(S8): 1661-1666.
- [7] Davalo, E, Naim, P. (1990). Des réseaux de neurones, Eyrolles, Paris.
- [8] Borret, P. et al, (1991). Réseaux de neurones artificiels : une approche connexionniste de l'intelligence artificielle, Teknea, Toulouse.
- [9] Abdi, H. (1994). Les réseaux de neurones, Presses Universitaires de Grenoble, Grenoble
- [10] Cross, S., Harrison, R.F., Kennedy, R.L. (1995). 'Introduction to neural networks', The Lancet 346: 1075 1079.
- [11] Haykin, S. (1994). Neural Networks. A Comprehensive Foundation. Macmillan, New York.
- [12] Shepard D. (1990)'. 'The new direct marketing', Business on Irwin Home Wood IL.
- [13] Cybenko, G. (1989). 'Approximation by superposition of a sygmoidal function'. Math.control systems signals, 2(4): 303-314.
- [14] Zeigler, B.P. (1976). Theory of modelling and simulation, Wiley, New York.
- [15] Dunkin, N and Shawe-Taylor, J and Koiran, P (1997).A new incremental learning technique. In: Marinaro, M andTagliaferri, R, (eds.) Neural Nets: WIRN Vietri-96: Proceedings of the 8th Italian Workshop on Neural Nets,

[1] loss of performance =performance- performance after removing the variable

Vietri sul Mare, Salerno, Italy, 23-25 May 1996. (pp. 112 - 118). Springer: New York, US.

[16]Wang J., Bø T.H., Jonassen I. (2003). 'Tumor classification and marker gene prediction by feature selection and fuzzy c-means clustering using microarray data', BMC bioinformatics, 4 (60).

[17]Wang W. and Zhang Y. (2007). 'On fuzzy cluster validity indices', Fuzz. Set and sys, 158 (19), pp.2095-2117, 2007

[18]Wang X., Wang Y., Wang L. (2004). 'Improving fuzzy c-means clustering based on feature-weight learning', Pattern Recognition Letters, 25, pp. 1123-1132.

[19]Gairard B., Mathelin, C., Schaffer, P. et al, (1998). 'Cancer du sein : épidémiologie, facteurs de risques, dépistage' Revue du Prat, 48 : 21-27.

[19]Cottrell M. and Rousset P. (1997). 'A powerful Tool for Analyzing and Representing Multidimensional Quantitative and Qualitative Data', In Proceedings of IWANN'97, pages 861-871, Springer Verlag, Berlin.

[19]Cottrell M., Fort J.C., Pagès G. (1998). 'Theoretical aspects of the SOM algorithm', Neuro Computing, 21, pages 119-138.

[19]Cottrell M., Fort J.C., Pagès G. (1995). 'Two or three things that we know about the Kohonen algorithm', in Proc of ESANN'94, M. Verleysen Ed., D Facto, Bruxelles, p.235-244.

[20]Mert, A., Kiliç, N. Z., Bilgili, E., & Akan, A, Breast cancer detection with reduced feature set. *Computational and Mathematical Methods in Medicine*. (2015., 1–11.

[21]Nahato, K. B., Nehemiah, H. K., & Kannan, A., Knowledge mining from clinical datasets using rough sets and backpropagation neural network. *Computational and Mathematical Methods in Medicine*, (2015) 1–11.

[22] Dheeba, J., Singh, N. A., & Selvi, S. T, Computer-aided detection of breast cancer on mammograms: A swarm intelligence optimized wavelet neural network approach, *Journal of Biomedical Informatics*(2014), 49, 45–52

[23] Erdem A.,Emre G., Erdal K.(2012) "A fast and adaptive automated disease diagnosis method with an innovative neural network model", *Neural Networks*33; 88–96, 2012.

[24] Marcano-cedeño.A, Quintanilla-Domínguez,J, Andina.D., "WBCD breast cancer database classification applying artificial metaplasticity neural network", *Expert Systems with Applications*,38; 9573–9579, 2011.

[25] Murat Karabatak, M. Cevdet. "An expert system for detection of breast cancer based on association rules and neural network", *Expert Systems with Applications*36; 3465–3469, 2009.

[26] Diorio, C. (2005). Les facteurs de croissance analogues µa l'insuline, les apports en vitamine D et en calcium et la densité mammaire. Thèse de doctorat, Université Laval, Québec

[27] Falkenberry, S., Legare, R. (2002). 'Risk factors for breast cancer'. *Obstetrics and gynecology clinics of north America*, 29(1): 159-172 (Allaitement maternel).

[28] Funahashi, K (1989). 'On the approximate realisation of continuous mapping by neural networks'. *Neural networks*, 2: 183-192.

[29] Hassibi, B. Stork, D.G. Solla, S.A., (1993). Second order derivatives for network pruning: optimal brain surgeon. *Advances in neural information processing systems*.

[30] Le Cun, (1987). Modèles connexionnistes de l'apprentissage. PhD Thesis, Université Pierre et Marie Curie.

[31] Sauguet, M. (2007). Parallélisations de problèmes d'apprentissage par des réseaux de neurones artificielles application en radiothérapie externe. Thèse de doctorat, université de Franche-Comté.

[32] Maciej, A. Mazurowski, Piotr A. Habas, Jacek M. Zurada, Joseph Y. Lo, Jay A. Baker, Georgia D. Tourassi (2009). 'Training Neural Network Classifiers for Medical Decision Making: The Effects of Imbalanced Datasets on Classification Performance', *Neural Network*, 21(2-3): 427–436.

[33] Rumelhart, D.E. Hinton G.E., and Williams R.J (1986). *Parallel distributed processing*, vol. 1-2. The MIT Press.

[34] Stoppigli, Idan, Y., Dreyfus, G., (1997). Neural network aided portfolio management., in *Industrial applications of neural networks* ; World Scientific.

[35] Geman,S., Bienenstock, E.,Doursat, R.(1992). 'Neural networks and the bias/variance dilemma'. *Neural Comp* 4: 1-58.

[36] Verma B., Novel network architecture and learning algorithm for the classification of mass abnormalities in digitized mammograms, *In: Artificial Intelligence in Medicine* (2008), pp. 4267-79.

Enhancing Intrusion Detection System by Reducing the False Positives through Application of Various Data Mining Techniques

Vivek Kshirsagar

Dept. of Computer Science and Engineering
Government College of Engineering
Aurangabad, Maharashtra, India

Dr. Madhuri Joshi

Dept. of Computer Science and Engineering
Jawaharlal Nehru Engineering College
Aurangabad, Maharashtra, India

Abstract— With the growth of cyber-attacks as observed over the last couple of decades safety, protection and privacy of information has become a major concern for organizations across the globe. Intrusion detection systems (IDSs) have thus gained important place and play a key role in detecting large number of attacks. There are a number of intrusion detection systems in market and most of them have the problem of having a relatively large number of false positives. Hence a need has arisen in the networking society of addressing the issue of false alarm and false positives and has resulted in an interest for researchers in IDS area. The main motivation of this research is in enhancing the performance of different data mining techniques to handle the alerts, reduce them and classify real attacks and reduce false positives. In this paper, the authors propose a novel hybrid model of RT and PART as to lower the rate of false positives. The algorithms are first trained for detecting attacks on KDD99 Dataset and then are tested on live traffic to classify whether the flow is normal or there are attacks. Random Tree (RT) and PART algorithms statistically validate the experimental results. The Hybrid framework on comparative analysis outperforms its counterparts and may lead to improved intelligent intrusion detection.

Keywords- C45, Detection rate, False Positives, intrusion detection, Random tree, Confusion matrix, PART

I. INTRODUCTION

The objective of intrusion detection system is to detect and try to prevent hostile attacks in the network

by malicious users (hackers). It relies on the ability to provide views of unusual activity and issuing alerts accordingly. The administrators can then take suitable actions by blocking or removing from network suspicious connections. The intrusion detection system should run continuously requiring minimal human supervision and withstand targeted malicious attacks[1]. It functions to monitor and resist local intrusion by utilizing minimal resources. It also adapts so as to function in large and fast networks. One key feature of the intrusion detection system is to have lower rate of false positives.

II. INTRODUCTION

The objective of intrusion detection system is to detect and try to prevent hostile attacks in the network by malicious users (hackers). It relies on the ability to provide views of unusual activity and issuing alerts accordingly. The administrators can then take suitable actions by blocking or removing from network suspicious connections. The intrusion detection system should run continuously requiring minimal human supervision and withstand targeted malicious attacks[1]. It functions to monitor and resist local intrusion by utilizing minimal resources. It also adapts so as to function in large and fast networks. One key feature of the intrusion detection system is to have lower rate of false positives.

III. INTRUSION DETECTION OVERVIEW

The data mining algorithm framework as shown in Fig 1 computes activity patterns from system audit data and extract predictive features from the patterns. Machine learning classification algorithms are then applied to the KDD Dataset for training purposes. Raw data is first captured in the form of packet and interpreted in the form of connection records containing a number of features, such as service, duration, source IP address, destination IP address etc. The anomaly detector detects intrusions. On classification of the packet or traffic by the selected classification algorithm, Alarm Manager signals an alarm to the appropriate action taking entity to perform accordingly. The model is validated based on the percentage of false positive attacks detected [2][3][4].

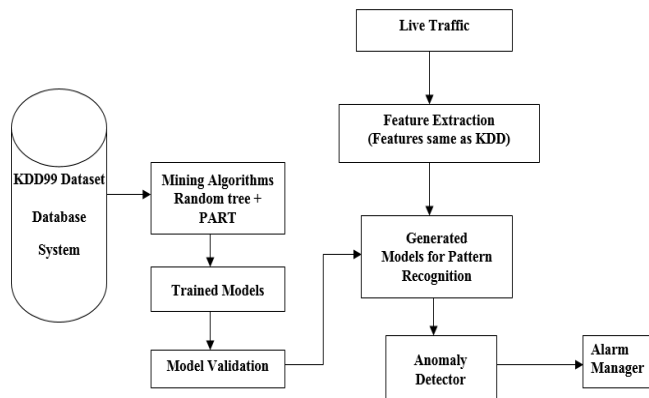


Figure 1. Architecture of Proposed system

IV. MATERIALS

The kddcup99 dataset [5] is a benchmark dataset which is originated by processing the tcpdump segment of DARPA 1998 evaluation dataset. The data set consists of 41 features and a separate feature (42nd feature) that labels the connection as normal or a type of attack. The data set contains a total of 24 attack types that fall into 4 major categories (DoS, Probe, R2L and U2R)

DOS (Denial of service): Denials-of Service attacks have the goal of limiting or denying services provided to the user, computer or Network [6]. It is usually done by making the resources either too busy or overflow, which as a consequence results in the disobedience of services requested by the legitimate users.

Probing: Probing or Surveillance attacks have the goal of gaining knowledge of the existence or configuration of a computer system or network [7].

U2R (User-to-Root): attacks are attempts by a non-privileged user to gain administrative privileges. [8] In the attack, users take advantage of system leak to get access to legal purview or administrators purview, such as: Buffer Overflow is among them

R2L (Remote-to-Local): attack is the kind of intrusion attack where the remote intruder consistently sends packets to a local machine with motive to expose the machine vulnerabilities and exploit privileges which a local user would have on the computer.

V. PROPOSED SYSTEM

The proposed system consists of various modules like Packet Capture, Feature selection, various classifier models, evaluation of classifiers, getting the best models after validation and finally proposing the best among all which in the authors case is the proposed hybrid model of RT+PART. The flow of the proposed system is depicted in Fig 2.

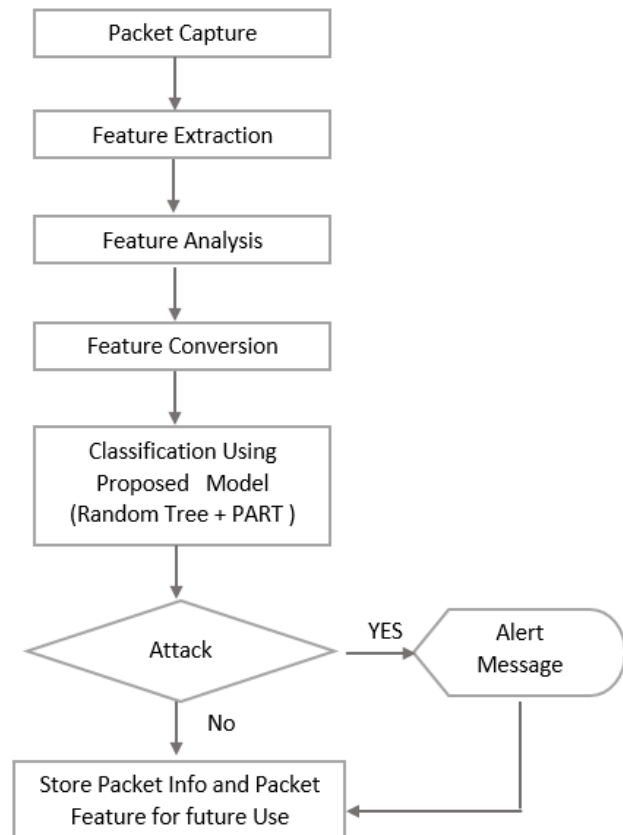


Figure 2. Flowchart of Proposed System

Steps in proposed hybrid algorithm are as follows

: Step 1: Input KDD Train dataset.

Step 2: Pre processing of the dataset.

Step 3: Generate classification model using PART algorithm.

Step 4: Evaluate Model using KDD Test Data Set.

Step 5: Generate classification model using Random Tree algorithm.

Step 6: Evaluate Model using KDD Test Data Set.

Step 7: Combine the models generated in step 3 and 5.

Step 8: Evaluate Model generated in step 7 using KDD Test Data Set.

A. Packet capture

Capture of packets is carried out by using Open Source Package named Jpcap. Jpcap is a Java library that uses the C library libpcap, for capturing and sending network packets. The traffic is logged in database for pattern matching by comparing those with the already defined signatures for labeled classification in an offline environment. The classification algorithm is implemented using NetBeans IDE, Java, and Weka. WinPcap is a tool available under windows for link-layer network access [8] the classified packets are indicated by providing separate color coding for valid and invalid packets. The authors have used MYSQL for offline storage. In our system, patterns are labeled based on criteria (TCP RFC standards) presented in following Table 1

Table 1 Flag conditions, Packet Validation and Recommended Action.

If	Validation	Action
ACK = 0 & FIN = 1	Invalid	DROP
ACK = 0 & PUSH = 1	Invalid	DROP
ACK = 0 & RST = 0 & SYN = 1	Invalid	DROP
ACK = 0 & URG = 1	Invalid	DROP
FIN = 1 & SYN = 1	Invalid	DROP
RST = 1 & SYN = 1	Invalid	DROP
ACK_V ALUE = 0 & ACK = 0	Invalid	DROP

B. Feature Selection

The data available for constructing the system consists of a large amount of packets of trained data and test data. The connections are in chronological order. Each connection is described by 40+ features. The features used for experimental analysis are listed in the Table 2.

The features are categorized as follows:[10][11]

TCP Features:

These features include the duration, protocol type, and service of the connection, as well as the amount of data transferred.

Login Features:

These features were derived from the payload of the TCP packets using domain knowledge. They include features like the number of failed login attempts and whether or not root access was obtained.

Time Stamp Features:

Calculated over a two second time interval, these features include things like the number of connections to the same host as the current connection and the number of connections to the same service as the current connection.

Host Traffic Features:

Similar to the time based traffic features, catching attacks of more than 2 seconds.

Table 2 Attributes used from KDD Dataset

KDD dataset Attributes	KDD dataset Attributes
duration	guest login
protocol_type	count
_service	srv count
flag	serror rate
_src_bytes	srv error rate
_dst_bytes	error rate
_land	srv error rate
wrong_fragment	same_srv_rate
_urgent	diff_srv_rate
_hot	srv_diff_host_rate
num_failed_logins	dst_host_count
_logged_in	dst_host_srv_count
num_compromised	dst_host_same_srv_rate
_root_shell	dst_host_diff_srv_rate
Su_attempted	dst_host_same_src_port_rate
_num_root	dst_host_srv_diff_host_rate
num_file_creations	dst_host_serror_rate
-- num_shells	dst_host_srv_serror_rate
-- num_access_files	dst_host_rerror_rate
num_outbound_cmds	dst_host_srv_error_rate
_is_host_login	attack

VI. ALGORITHMS AND TECHNIQUES USED FOR EXPERIMENTATION

A. J48

J48 is an implementation of C4.5 algorithm [9]. C4.5 was an earlier version of this algorithm developed by J. Ross Quinlan. According to Zhao and Zhang [10], C4.5 algorithm produce decision tree classification for a given dataset by recursive division of the data and the decision tree is grown using Depth-first strategy. The entropy measure information gain value is calculated for each of the attribute and the attribute with the highest information gain becomes the root node and the other attributes are child nodes in succession depending on their values of information gain. The algorithm stops when there are no more attributes left for splitting the nodes further. Confusion matrix for J48 classifier is shown in table 3.

Table 3 Confusion Matrix for J48 Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
223574	5739	480	0	60	DOS
84	60246	8	17	236	NORMAL
1	183	26	12	6	U2R
4	12759	10	1100	231	R2L
184	607	1	4	337	PROBE
				0	

B. REPTree

Reduced Error Pruning Tree "REPT" is a fast decision tree learning and it builds a decision tree based on the information gain same as in J48. The basic of pruning of this algorithm is it uses reduced error pruning (REP) with backfitting. Confusion matrix for REP Tree classifier is shown in Table 4.

Table 4 Confusion Matrix for REPTree Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
223688	6147	0	0	18	DOS
70	60281	1	12	227	NORMAL
19	192	7	6	4	U2R
1	14788	114	948	340	R2L
314	710	0	0	314	PROBE
				2	

C. Part

PART algorithm [11] is relatively simple algorithms which combines the divide and conquer strategy with separate and conquer strategy. It builds a decision tree and forms a rule, removes the instances covered by the rule and continues to create a recursive rule for rest of the instances until there are no longer any instances left. Furthermore Eibe and Witten [11] said, the algorithm produces sets of rules called decision lists which are ordered set of rules. A new instance is compared to each rule in the list in turn, and the instance is assigned the category of the first matching rule (a default is applied if no rule successfully matches). Confusion matrix for PART classifier is shown in Table 5.

Table 5 Confusion Matrix for PART Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
222904	5424	330	275	920	DOS
427	59530	8	6	620	NORMAL
0	193	23	12	0	U2R
8	11755	451	1569	2406	R2L
288	528	5	285	3060	PROBE

D. JRip

JRip popularly known as Repeated Incremental Pruning to Produce Error Reduction (RIPPER) is one of the basic and most popular algorithms [12]. In this algorithm the five attack Classes are examined in increasing size and an initial set of rules for each class is generated using incremental reduced error i.e. growing of one rule by adding combination of attributes in the antecedents to the rule. Here all possible values of each attributes get tested and then the rule is finalized. Similarly pruning step also results in dropping attributes from antecedents until the minimum possible attributes are remaining to generate the rule. The rules are selected based on information gain. The algorithm terminates on generation of rules for the five attack classes. The strategy of replacing and revising the rules hence improves the accuracy of the generated rules. Confusion matrix for JRip Tree classifier is shown in Table 6.

Table 6 Confusion Matrix for JRip Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
223281	5860	386	0	326	DOS
71	60169	8	4	339	NORMAL
0	158	39	4	27	U2R
2	15403	49	731	4	R2L
314	619	4	75	3154	PROBE

Table 8 Confusion Matrix for Random Tree Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
216830	12450	0	75	498	DOS
69	59581	4	11	926	NORMAL
0	183	25	12	8	U2R
0	14440	9	1734	6	R2L
150	911	0	253	2852	PROBE

E. Random Forest

A Random Forest is a collection of decision trees. Here all the decision trees take part for voting in classifying the attack types [13]. This method follows randomness first, at the creation of each tree, a random subsample of the total instances is selected to grow the tree and second, at each node of the tree, features are randomly chosen as a “splitter variable”. The splitter variable attempts to separate instances from those in the other class. The tree is grown with additional splitter variables until all terminal nodes (leaves) of the tree are purely one class or the other. The correlation between all the decision trees is reduced by randomness principle at both the steps which results in improving the prediction power and hence higher efficiency. Confusion matrix for RandomForest classifier is shown in Table 7.

Table 7 Confusion Matrix for Random Forest Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
224068	5778	0	0	7	DOS
224	60122	9	6	230	NORMAL
0	202	15	8	3	U2R
1159	13515	5	1508	2	R2L
232	549	0	283	3102	PROBE

F. Random Tree

Random Tree: It was introduced by Leo Breiman and Adele Cutler. It is suitable for both classification and regression problems. The steps in the algorithm are as follows: (1) Input feature vector(in our case the 40 features from KDD Dataset) (2) Build trees by using not all the input features but only a random subset. For each node a new subset is generated. The trees built are not pruned. (3) The classification is done by every tree and that class label is output which has majority of votes. In this way all the instances are classified. Confusion matrix for Random Tree classifier is shown in Table 8.

G. Nearest Neighbour

In k nearest neighbor algorithm all the available instances are stored and then accordingly for each new instance is classified based on similarity measure which in our case is the Euclidean distance function with k=1. Here as k=1 the instances gets assigned to the attack class of its nearest neighbor. Confusion matrix for Nearest Neighbor classifier is shown in Table 9.

Table 9 Confusion Matrix for NearestNeighbour Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
216830	12450	0	75	498	DOS
69	59581	4	11	926	NORMAL
0	183	25	12	8	U2R
0	14440	9	1734	6	R2L
150	911	0	253	2852	PROBE

H. Hoeffding Tree

It is a decision tree learning method. The steps in the algorithm are as follows:-

Build decision tree using hoeffding bound. The hoeffding bound gives the confidence value of the best attribute to split the tree. It is useful to build the tree based on the instances observed. Here the difference between top two values of information gain for two attributes is calculated.

Confusion matrix for Hoeffding Tree classifier is shown in Table 10.

Table 10 Confusion Matrix for Hoeffding Tree Classifier

ATTACK TYPES					
DOS	NORMAL	U2R	R2L	PROBE	Attack Classified As
222200	7408	0	0	245	DOS
1443	58950	39	0	159	NORMAL
0	61	27	0	140	U2R
2	15752	428	2	4	R2L
2102	430	3	286	1325	PROBE

VII. EVALUATION METRICS

True positive: It is defined that the attack is correctly classified.

$$TPR=TP/(TP+FN) \quad (1)$$

False Negative: It occurs when the attack is incorrectly predicted as negative when it is actually positive. False positive: It occurs when the attack is incorrectly predicted as yes when in reality it should be no. [14][15]

$$FPR=FP/(TN+FP) \quad (2)$$

Accuracy: It is defined by the following formula:-

$$Accuracy=TP/(TP+FP) \quad (3)$$

Since the class distribution is unbalanced, it is important to use a performance measure that takes class imbalance into account. The authors use the measure of Kappa Statistic due to Cohen [16]. The value of kappa statics is given by the formula as:-

$$K=D_{OBSERVED}-D_{RANDOM}/D_{PERFECT}-D_{RANDOM} \quad (4)$$

VIII. EXPERIMENTATION AND RESULTS DISCUSSIONS

All the six classifiers were trained using 572798 number of instances and tested using 311027 instances. The experiment was conducted on desktop computers of Intel Dual Core processor with 4 GB RAM PC with Windows 7 as operating system. Kappa Statistic results are good enough for the classifiers J48, JRip, PART and Random forest as shown in the Table 11.

Table 11 Values of Kappa statistic for different Classifiers

Classifier model	Kappa statistic
J48	0.8224
JRip	0.8271
NN	0.8175
PART	0.8253
Random Forest	0.8192
REPTree	0.8161
RandomTree	0.7751

As seen from the table above the classifier model PART gives the best value of k among all and hence in our hybrid model PART is proposed along with combination of Random Tree which also illustrates acceptable k value.

The figure 3 depicts the instances class being predicted correctly by the various classifiers.

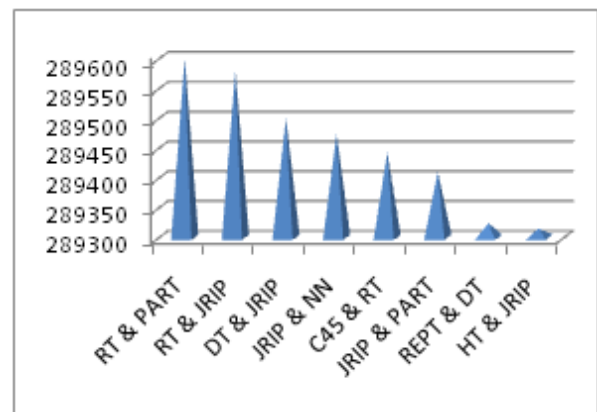


Figure. 3 Number of Correctly Classified Instances

The following figure 4 illustrates the instances class predicted incorrectly by the different classifiers.

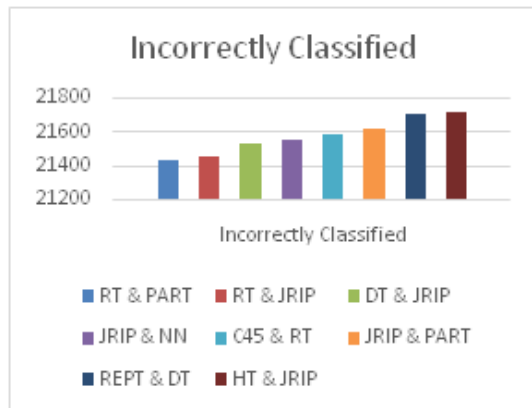


Figure. 4 Number of Incorrectly Classified Instances

Table 12 Time Required To Test the KDD CUP Test Data Set.

Combination	Time taken (millisecond)
RT & JRIP	26707
RT & PART	26882
DT & JRIP	26898
JRIP & NN	27152879
C45 & RT	25546
JRIP & PART	27778
REPT & DT	25432
HT & JRIP	27800

The figures (5-8) depict the attacks as detected by the various algorithms.

When the developed framework is compared with the respective various available data mining techniques

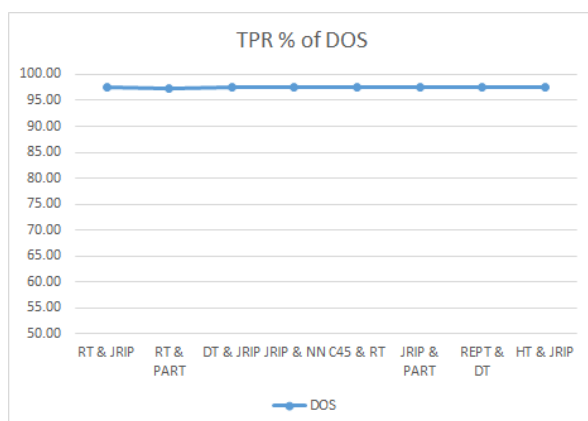


Fig. 5 TPR % of DOS

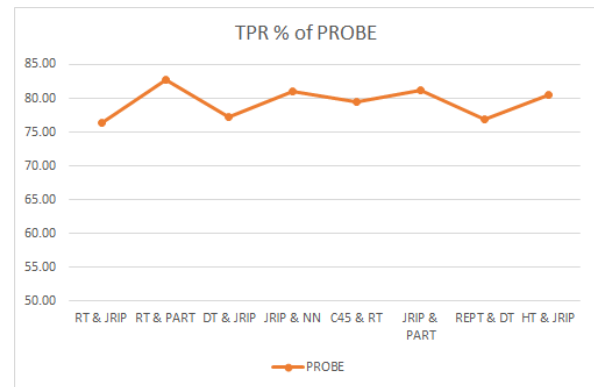


Fig. 6 TPR % of PROBE

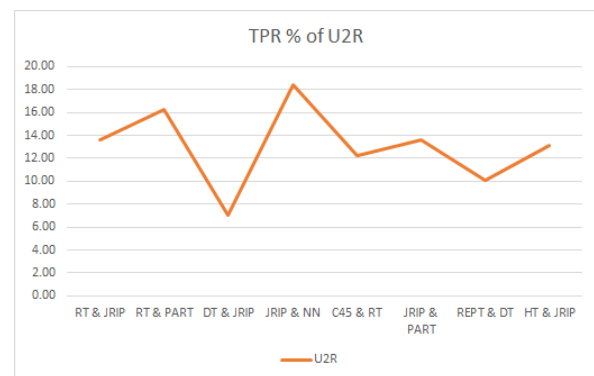


Fig. 7 TPR % of U2R

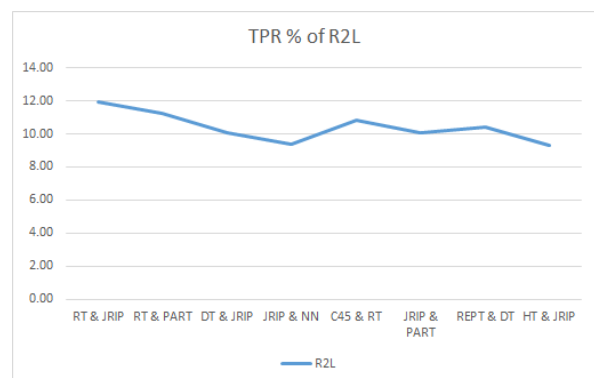


Fig. 8 TPR % of R2L

Table 13 Memory Requirement for Each Classification

Combination	Model file Size In bytes	Model file Size in Mega bytes
RT & JRIP	131,967	128.8740234
RT & PART	563,697	550.4853516
DT & JRIP	235,246	229.7324219
JRIP & NN	187,241,111	182852.6475
C45 & RT	246,920	241.1328125
JRIP & PART	542,252	529.5429688
REPT & DT	259,548	253.4648438
HT & JRIP	2,096,529	2047.391602

Table 14 Time Required for Testing the KDD CUP Test
Data Set

Combination	Time taken (millisecond)
RT & JRIP	26707
RT & PART	26882
DT & JRIP	26898
JRIP & NN	27152879
C45 & RT	25546
JRIP & PART	27778
REPT & DT	25432
HT & JRIP	27800

The classifiers were used in various combinations among themselves the result of which is shown in the Table 15-17. From all of the combinations the proposed model of RT and PART gave the best result as compared with others

Table 15: Classwise Number of attacks detected using combination of algorithms for DOS and PROBE

Combination	DOS		PROBE	
	CORRECT	INCORRECT	CORRECT	INCORRECT
C45 & RF	224002	5851	3325	841
C45 & RT	223998	5855	3308	858
C45 & HT	223700	6153	3473	693
C45 & REPT	223996	5857	3247	919
C45 & DT	224009	5844	3238	928
C45 & JRIP	224080	5773	3258	908
C45 & PART	223698	6155	3388	778
C45 & NN	224130	5723	3406	760
RF & RT	223961	5892	3326	840
RF & HT	223946	5907	3492	674
RF & REPT	223958	5895	3269	897
RF & DT	224274	5579	3363	803
RF & JRIP	224080	5773	3286	880
RF & PART	223958	5895	3393	773
RF & NN	224079	5774	3368	798
RT & HT	223785	6068	3379	787
RT & REPT	223873	5980	3167	999
RT & DT	217745	12108	3155	1011
RT & JRIP	224079	5774	3183	983
RT & PART	223946	5907	3445	721
RT & NN	223767	6086	3248	918
HT & REPT	223793	6060	3314	852
HT & DT	223727	6126	3422	744
HT & JRIP	224083	5770	3357	809
HT & PART	223596	6257	3582	584
HT & NN	223758	6095	3524	642
REPT & DT	224119	5734	3202	964
REPT & JRIP	224080	5773	3108	1058
REPT & PART	223921	5932	3373	793
REPT & NN	224044	5809	3363	803
DT & JRIP	224361	5492	3215	951
DT & PART	223916	5937	3440	726
DT & NN	224159	5694	3350	816
JRIP & PART	224076	5777	3383	783
JRIP & NN	224203	5650	3374	792
PART & NN	224096	5757	3471	695
KDD CUP	223226	6627	3471	695

Table 16: Classwise Number of attacks detected using
combination of algorithms for R2L and U2R

Combination	R2L		U2R	
	CORRECT	INCORRECT	CORRECT	INCORRECT
C45 & RF	1285	14904	9	219
C45 & RT	1751	14438	28	200
C45 & HT	948	15241	30	198
C45 & REPT	1579	14610	26	202
C45 & DT	1063	15126	7	221
C45 & JRIP	1581	14608	19	209
C45& PART	1441	14748	30	198
C45 & NN	1275	14914	44	184
RF & RT	1744	14445	27	201
RF & HT	891	15298	27	201
RF & REPT	1575	14614	23	205
RF & DT	1005	15184	4	224
RF & JRIP	1522	14667	15	213
RF & PART	1232	14957	26	202
RF & NN	1019	15170	39	189
RT & HT	1735	14454	38	190
RT & REPT	1880	14309	35	193
RT & DT	1735	14454	25	203
RT & JRIP	1934	14255	31	197
RT & PART	1824	14365	37	191
RT & NN	1753	14436	44	184
HT & REPT	1569	14620	34	194
HT & DT	119	16070	27	201
HT & JRIP	1508	14681	30	198
HT & PART	1101	15088	35	193
HT & NN	732	15457	48	180
REPT & DT	1683	14506	23	205
REPT & JRIP	1657	14532	28	200
REPT& PART	1624	14565	37	191
REPT & NN	1577	14612	48	180
DT & JRIP	1625	14564	16	212
DT & PART	1216	14973	26	202
DT & NN	848	15341	39	189
JRIP & PART	1631	14558	31	197
JRIP & NN	1518	14671	42	186
PART & NN	1246	14943	44	184
KDD CUP	1360	14829	30	198

Table 17: Classwise Number of attacks detected using
combination of algorithms for NORMAL

Combination	NORMAL	
	CORRECT	INCORRECT
C45 & RF	60304	287
C45 & RT	60357	234
C45 & HT	60341	250
C45 & REPT	60313	278
C45 & DT	60299	292
C45 & JRIP	60288	303
C45 & PART	60291	300
C45 & NN	60339	252
RF & RT	59681	910
RF & HT	59606	985
RF & REPT	59583	1008
RF & DT	60292	299
RF & JRIP	60305	286
RF & PART	60301	290
RF & NN	60222	369
RT & HT	59682	909
RT & REPT	59669	922
RT & DT	60319	272
RT & JRIP	60353	238
RT & PART	60349	242
RT & NN	60258	333
HT & REPT	59595	996
HT & DT	60313	278
HT & JRIP	60337	254
HT & PART	60332	259
HT & NN	60219	372
REPT & DT	60297	294
REPT & JRIP	60309	282
REPT & PART	60312	279
REPT & NN	60218	373
DT & JRIP	60283	308
DT & PART	60287	304
DT & NN	60330	261
JRIP & PART	60289	302
JRIP & NN	60337	254
PART & NN	60329	262
KDD CUP	60262	329

When the developed framework is compared with the respective various available data mining techniques for intrusion detection, the resultant obtained shows the favorable opinion to opt as the hybrid technique. This result is depicted in the following comparison graph.

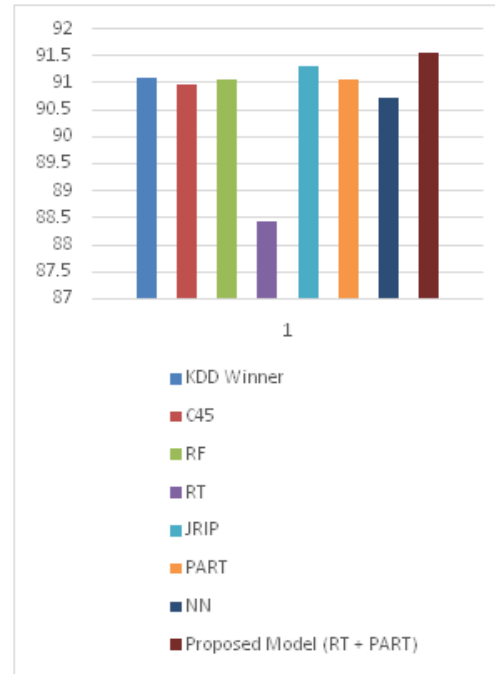


Figure. 9 Accuracy comparisons of various data mining-based IDS Models

The following figure illustrates the false positive rate of the various methods.

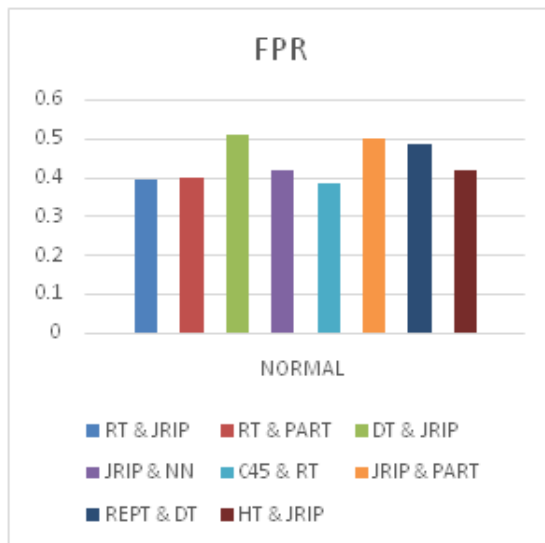


Figure. 10 Comparison of FPR

IX. CONCLUSION

The aim of the research was to enhance the performance of intrusion detection system by applying different classification algorithms. For choosing an appropriate classification algorithms there is a need to take into account the accuracy of classification. In order to understand the accuracy there should be an insight about the circumstances of misclassification of instances that will significantly affect the quality of various classifiers. Overall the proposed method RT and PART produces high accuracy of classification. In the proposed model the instance is classified as attack if any of the two classifiers categorize it as attack. The advantage of the proposed model results in checking by both the classifiers and hence enhances the performance of the intrusion detection system by controlling false positive rate. The entire network intrusion detection framework is developed using WEKA environment with java packages. The KDD dataset was used to train and test the classifiers for the 5-classes (normal, dos, probe, u2r and r2l). Once the algorithms were trained they were used to detect attacks from live traffic.

REFERENCES

- [1] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, in Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009 (2009)
- [2] Z. Jiuhua, in Knowledge Discovery and Data Mining, 2008.

- WKDD 2008. First International Workshop on (IEEE, 2008), pp. 402–405
- [3] W. Lee, S.J. Stolfo, in Usenix Security (1998)
- [4] R.G.M. Helali, in Novel Algorithms and Techniques in Telecommunications and Networking (Springer, 2010), pp.501–505
- [5] Kddcup99 dataset.
<http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (1999)
- [6] F. Jemili, M. Zaghdoud, M. Ben Ahmed, in Intelligence and Security Informatics, 2007 IEEE (IEEE, 2007), pp. 66–70
- [7] M. Panda, M.R. Patra, International journal of computer science and network security 7(12), 258 (2007)
- [8] A.A. Olusola, A.S. Oladele, D.O. Abosede, in Proceedings of the World Congress on Engineering and Computer Science, vol. 1 (2010), vol. 1, pp. 20–22
- [9] W.N.H.W. Mohamed, M.N.M. Salleh, A.H. Omar, in Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference on (IEEE, 2012), pp. 392–397
- [10] Y. Zhao, Y. Zhang, Advances in Space Research 41(12), 1955 (2008)
- [11] E. Frank, I.H. Witten, Proceedings of the Fifteenth International Conference (1998)
- [12] F. Leon, M.H. Zaharia, D. Gâlea, in Proceedings of the 8th international symposium on automatic control and computer science (2004)
- [13] L. Breiman, Machine learning 45(1), 5 (2001)
- [14] T. Pietraszek, A. Tanner, Information Security Technical Report 10(3), 169 (2005)
- [15] J. Baayer, B. Regragui, A. Baayer, Journal of Information Security 2014 (2014)
- [16] J. Cohen, et al., Educational and psychological measurement 20(1), 37 (1960)

AUTHORS PROFILE

Mr. Vivek Kshirsagar : received his B.E. and M.E. degrees in Computer Science and Engineering from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, 1993 and Technical Teachers Training Institute, Chandigarh, 2001; India. He is currently serving as Head of Department for both Computer Science and Engineering Department and Masters of Computer Applications Department. He has published about 50 papers in conferences and journals. His research interest covers Networking and Data Mining. He is member of CSI.

Dr. Madhuri. Joshi : completed her BE from College of Engineering, Pune (1985), M.Tech. (CS) (1993) from IIT, Madras and Ph.D. from SRT University, Maharashtra, India. She has published 29 research papers in various International Journals, International and National Conferences. Her areas of interest are Data Mining, Image Processing and Pattern Recognition. She is a member of ACM, IEEE, IAENG and CSI.

Bit Error Rate Performance Analysis of Channel Estimated Adaptive OFDM System

Srinu Pyla
Assistant Professor
G V P College of Engg. (A)
Visakhapatnam, India

Dr. K Padma Raju
Professor & Director of DAP
J N T U University
Kakinada, India

Dr. N. Bala Subrahmanyam
Professor & HOD
G V P College of Engg. (A)
Visakhapatnam, India

Abstract: Modern communication systems are designed to support multiple applications such as data, voice, video and multimedia transmission, hence they require high data rate, spectral efficiency and inter symbol interference (ISI) free transmission. Orthogonal frequency division multiplexing (OFDM) meets the above requirements but fluctuations in Signal to Noise Ratio is quite common due to variations in envelope of OFDM signal which degrades system performance. System performance can be improved either by using Space time coding or Adaptive modulation (AM) schemes. In this work, adaptive modulation is considered due to its low complexity and optimum spectrum utilization over space time coding. In this scheme, channel state information (CSI) is fed to the transmitter to adopt the order of modulation in order to maintain constant bit error rate (BER) irrespective of the channel conditions. Here channel estimation has done using Least Square (LS), Minimum Mean Square Error (MMSE) and interpolation along with comb type pilot symbol assisted channel estimation algorithms. In this work, a new scheme has implemented to improve the BER performance by integrating channel estimation and adaptive modulation and this new scheme results superior performance over individual methods.

Keywords: Bit Error Rate (BER), Channel Estimation, Comb type pilot, Least Square (LS), Minimum Mean Square Error (MMSE), adaptive modulation and Signal to Noise Ratio (SNR) .

I. INTRODUCTION

Modern communication systems are designed to support multiple applications such as data, voice, audio, video and multimedia transmission, and therefore they require high data rate, spectral efficient and inter symbol interference (ISI) free transmission [8]. Orthogonal frequency division multiplexing (OFDM) meets the above requirements and also provides multipath fading free transmission but fluctuations in Signal to Noise Ratio is quite common due to variations in envelope of OFDM signal and causes system performance degradation [6]. Because of its numerous advantages, OFDM widely used in many applications such as wireless local area networks, terrestrial digital video broadcasting, Wi-Max, LTE-Advanced etc... [12].

In wireless multipath propagation, the transmitted signal undergoes many reflections due to presence of several objects in the transmission path and multiple versions of the transmitted signal receive at different time intervals [8], and leads to fluctuations in Signal to Noise Ratio and increases

bit error rate. BER can be controlled either by using Space time coding or Adaptive Modulation schemes.

For implementation of adaptive modulation communication system, channel state information (CSI) is required. Moreover the transfer function of the channel in OFDM looks unequal both in time and frequency domains. Hence dynamic channel estimation is required [1]. The most popular channel estimation scheme is pilot channel estimation and can be performed mainly in two ways, one is either by inserting pilot tones into each subcarrier of OFDM symbols (block type pilot) or by inserting pilot tones into each OFDM symbol (comb type pilot) [5]. Block type pilot is efficient in case of slow fading channel and comb type pilot is beneficial in frequency selective fading channel [4, 7]. BER performance of comb type is better over block type [3]. In addition to these schemes there are several techniques for channel estimation such as Adaboost, Blue, LS, MMSE, Interpolation, recursive least square (RLS) etc. Many of the channel estimation schemes for OFDM are under the assumptions of a slow fading channel in which the transfer function of the channel is being stationary but in practical scenario it is time varying. So in such a case the channel parameters estimation is preferable in every OFDM data block [2].

In this paper, channel estimation at pilot frequencies has being carried out using comb type pilot arrangement through LS, MMSE and at data frequencies channel interpolation is using linear, spline and cubic. The performance of all schemes have been compared by measuring bit error rate with M- ary PSK and QAM digital modulation schemes by considering additive white Gaussian noise (AWGN) channel. For further improvement of BER performance a new scheme is implemented by integrating channel estimation and adaptive modulation. Adaptive modulation is famous for efficient spectrum utilization and moreover it maximizes linkup time, information rate and minimizes transmission errors. The results show the BER performance of this integrated scheme is superior over individual methods

This paper is organized as follows. In section II OFDM system with channel estimation is described. Section III discusses various channel estimation algorithms. Section IV describes adaptive modulation. Section V describes proposed method i.e adaptive OFDM with channel estimation. Simulation results are shown in Section VI. Finally the

conclusion of the paper is given in section VII.

II. SYSTEM DESCRIPTION

Pilot symbol based channel estimation adaptive OFDM is represented in the following figure.

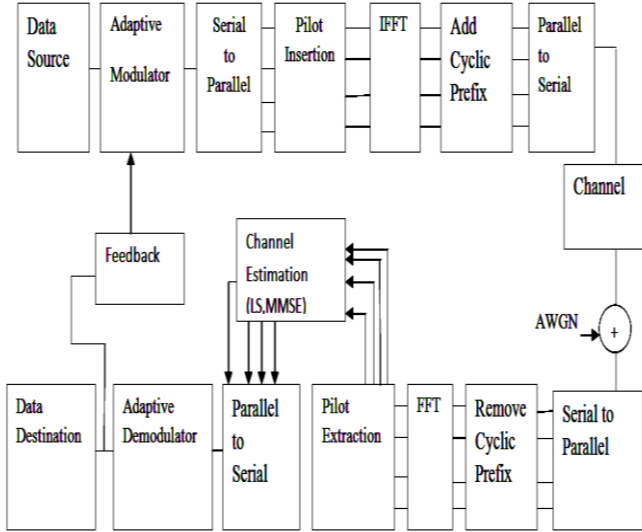


Figure 1: Channel Estimation and adaptive modulation in OFDM system

The digital data is first grouped, mapped into M-ary PSK, QAM symbol, converted into parallel stream, pilot symbols are inserted into symbols of the mapper and applied to inverse fast fourier transform in order to keep the subcarriers orthogonal to one another. Various Pilot patterns are discussed in the subsequent sections.

The IFFT output is expressed as

$$x(n) = IFFT\{X(K)\} = \frac{1}{N} \sum_{k=0}^{N-1} X(K) e^{j2\pi nk/N} \quad (1)$$

$X(K)$ = Input to IFFT (subcarriers)

$x(n)$ = output of IFFT (orthogonal subcarriers)

$n=0, 1, 2, 3, \dots, N-1$

N is the total number of subcarriers.

The proper guard interval is inserted between OFDM symbols to prevent the possible inter-symbol interference and guard interval OFDM symbol $x_g(n)$ is transmitted through additive white Gaussian noise channel and the received signal $y_g(n)$ is

$$y_g(n) = x_g(n) * h(n) + w(n) \quad (2)$$

Where $h(n)$ is channel impulse response

$W(n)$ is additive white Gaussian noise

At the receiver, first serial to parallel conversion is performed, the guard interval is eliminated from $y_g(n)$ and the received symbols $y(n)$ are applied to the Fast Fourier Transform (FFT) block to perform inverse transform.

$$Y(K) = FFT\{y(n)\} = \sum_{n=0}^{N-1} y(n) e^{-j2\pi nk/N} \quad (3)$$

For $k=0, 1, 2, \dots, N-1$,

$$Y(K) = X(K) H(K) + W(K) \quad (4)$$

Where $Y(K)$ = FFT output

$X(K)$ = Input signal stream

$W(K)$ = FFT $\{w(n)\}$, which is the additive white gaussian noise.

$H(K)$ = Channel Transfer Function.

The pilot symbols are extracted from the obtained sequence $Y(K)$. The extracted pilot symbols are denoted by $Y_p(K)$. Every p^{th} subcarrier contains known pilot symbols, $X_p(K)$. With the help of known pilot symbols $X_p(K)$ and the received pilot symbols $Y_p(K)$, the channel state information is estimated and is given by

$$H_p(K) = \frac{Y_p(K)}{X_p(K)} + Z_p(K) \quad (5)$$

Where $H_p(K)$ is the channel estimate at the pilot symbols. After demodulation the binary data is re-constructed at the receiver.

III. CHANNEL ESTIMATION

In communication systems bit error rate can be reduced by knowing the channel state information and feeding it to the transmitter. In order to estimate the channel state, block type or comb type pilot symbol patterns can be used. The pilot symbols may be random data or complex value [9,10]. In this paper random data multiplied with a constant is considered as it reduces computational complexity. In comb type pilot arrangement the N_p pilot symbols are uniformly inserted into the $X(K)$ subcarriers. Here pilot symbols are introduced in the first position of every subcarrier.

$$X(K) = X(ml + l) = \begin{cases} x_p(m), & l = 0 \\ \text{information data}, & l = 1, \dots, L-1 \end{cases} \quad (6)$$

Where $L = \frac{\text{Number of Carriers}}{N_p}$ and $x_p(m)$ is the m^{th} pilot carrier value.

The relationship between the transmitted pilot symbols $X_p(K)$ and the received pilot symbols $Y_p(K)$ after transmitting through the channel is given by

$$Y_p(K) = X_p(K) H_p(K) + Z_p(K) \quad (7)$$

Where $H_p(K)$ is the channel response of pilot symbols.

In case of comb type based pilot arrangement the Least Square Channel Estimation (LS) is obtained by dividing the received pilot sequence with the transmitted pilot sequence.

$$H_{LS} = \frac{Y_p(K)}{X_p(K)} \quad (8)$$

Least Square (LS) Channel estimation improves the BER performance but it is prone to gaussian noise and inter-carrier interference (ICI) [1]. The channel responses of

data subcarriers can be obtained by interpolating the channel responses of the pilot symbols (subcarriers), the performance of the OFDM system using comb type based channel estimation depends on the rigorousness of the estimated pilot symbols. Hence better channel estimation is required. MMSE overcomes this problem and provides improved BER performance over LS channel estimation at the cost of computational complexity. It tries to minimize the expected mean square error between the actual and estimated channel [11].

$$H_{MMSE} = (((R_h + \sigma^2 I)^{-1})r)H^{\wedge} \quad (9)$$

R_h = Auto correlation matrix of the channel at pilot locations,

σ^2 = Noise Variance per Subcarrier

r = Cross Correlation Vector of the channel at Subcarrier locations and Pilot locations.

H^{\wedge} = Channel estimate at pilot symbols.

Here BER performance for various interpolation schemes such as FFT, Linear, and Spline is compared.

IV. ADAPTIVE MODULATION

The main purpose of using adaptive modulation is to increase the number of bits per symbol thereby enhancing the throughput. Adaptive Modulation allows a wireless system to choose suitable order of modulation according to the channel condition [13]. This automatic adaptation of modulation order improves the throughput, spectral efficiency, controls the bit error rate and provides satisfactory system performance. Hence this is one of the promising approaches to 4G applications. In conventional OFDM system i.e with only one modulation scheme, either performance or throughput should be compromised. But in adaptive OFDM both throughput and performance are enhanced.

For proper communication over fading radio channels, adaptive modulation is the perfect choice. In general adaptive approaches are of three types namely adaptive modulation, adaptive subcarrier selection and adaptive power allocation. In adaptive modulation scheme, based on the signal to noise ratio at the receiver, order of the modulation at the transmitter is automatically adopted in order to maintain desired bit error rate. In adaptive sub carrier selection, the deep faded sub carriers are identified and then the information in those carriers is transmitted using healthy subcarriers in the next transmission. In adaptive power allocation method, deep faded carriers are identified, extra power is applied to the deep faded carriers and then information is transmitted. In this work the first method is considered to improve the system performance in terms of bit error rate. In adaptive systems SNR estimation is very important as switching of modulation order is based on SNR at the receiver. For implementation of adaptive modulation, predefined threshold levels of SNR for each order of modulation should be assigned.

To obtain switching thresholds for individual modulation schemes, the system is first performed with individual modulation schemes and corresponding BERs and SNRs are determined. Based on these values, switching ranges for particular order of modulation schemes are fixed according

to the targeted BER. At good channel conditions higher order modulation schemes (32, 64, 128, ... QAM or PSK), at bad conditions lower order schemes (BPSK, 4QAM or QPSK) and at moderate conditions medium order modulation schemes (8, 16 QAM or PSK) are selected in order to maintain desired BER performance. This process improves overall system performance in terms of throughput and bandwidth efficiency.

V. PROPOSED METHOD: ADAPTIVE MODULATION WITH CHANNEL ESTIMATION

In the proposed method the concept of adaptive modulation is integrated with channel estimation schemes. Figure I shows the schematic block diagram of channel estimated adaptive OFDM system and the operational flow chart of this system is shown in figure II. In this scheme the SNR of channel estimated OFDM symbol is feeding back to the transmitter. Based on the SNR value at receiver, the channel condition is estimated and order of modulation is selected at the transmitter. It improves system performance in terms of throughput, spectral efficiency and bit error rate performance. Since both channel estimation and adaptive modulation schemes improve system performance individually, the integrated system still improves the system performance. Here the advantage of channel estimation and adaptive modulation scheme jointly still improves the OFDM system performance. Hence the channel estimated adaptive OFDM system performance is superior over individual channel estimation and adaptive modulation schemes.

From the results (figures XIII and XVI) it is observed that the proposed system i.e channel estimated adaptive OFDM performance is superior over individual schemes. The combination of MMSE channel estimation and adaptive modulation performance (figure XV) is far better over other combinations. This system is also implemented in multipath environment and the results are plotted in figure XIV.

VI. SIMULATION RESULTS

In this work OFDM system is implemented with 512 subcarriers, digital modulator, AWGN channel with multiple reflection paths, and channel estimators. BER performance is analyzed for various digital modulation schemes, LS, MMSE, interpolation channel estimations, adaptive modulation and integrated channel estimated adaptive OFDM system. The BER performance is compared between

- i. LS-M-ary PSK vs LS-M-ary QAM (fig. V)
- ii. LS vs MMSE (fig. IX)
- iii. MMSE vs MMSE AM for M-ary QAM (fig. XIII)
- iv. Without and with channel estimation (fig. XI)
- v. Multipath channel with different taps (fig. XIV)
- vi. AM-LS and AM – MMSE (fig. XV)
- vii. Superior performance of AM -MMSE over other schemes (XVI)

Figures III & IV indicate the BER performance of M-ary PSK and M-ary QAM for LS channel estimated OFDM system and figure V gives the comparison of BER performance between these modulation schemes. Figures VI & VII demonstrate BER performance of M-ary PSK and M-ary QAM for MMSE channel estimated OFDM system and figure VIII gives the comparison of BER performance between M-ary PSK and M-ary QAM of this system. From figures V & VIII, it is observed that the BER performance of M-ary QAM is better over M-ary PSK for the same throughput and the performance degrades with increase in the order of modulation. From figures IX, X & XI, it is clear that the BER performance of MMSE is better over LS channel estimation. In figure XI, for BER 10^{-4} , SNR for LS channel estimated OFDM is 16dB whereas for MMSE channel estimated OFDM, SNR is 13.5dB at the same BER. Channel interpolation is applied at data frequencies using fft, spline and linear methods with 16QAM modulation and the result are shown in figure XII. From this figure it is clear that interpolation schemes provide better BER performance with little bit complexity over LS and MMSE pilot based channel estimation. The reason for complexity in case of interpolation schemes is, SNR estimation is required for every data symbol but in case of pilot based schemes SNR estimation is required at pilot carriers only. Figure XIII demonstrates the comparison of BER performance of OFDM system with adaptive modulation for different order of QAM modulation with single tap that is no multipath propagation is considered.

Figure XIV demonstrates BER performance of OFDM system with multiple reflections. Here tap number indicates multiple reflections. Increase in number of reflections, decreasing the BER performance. Figure XV compares the performance of LS channel estimated adaptive OFDM and MMSE channel estimated OFDM system and from the obtained graph it is observed that MMSE Adaptive OFDM performance is superior. In figure XVI, the BER performance of MMSE channel estimated adaptive OFDM system is compared and from this graph it is observed that MMSE adaptive OFDM system performance is superior over MMSE OFDM system. Desired OFDM system design parameters are given in table I. SNR threshold level ranges for fixed (individual) modulation schemes (M –ary PSK and

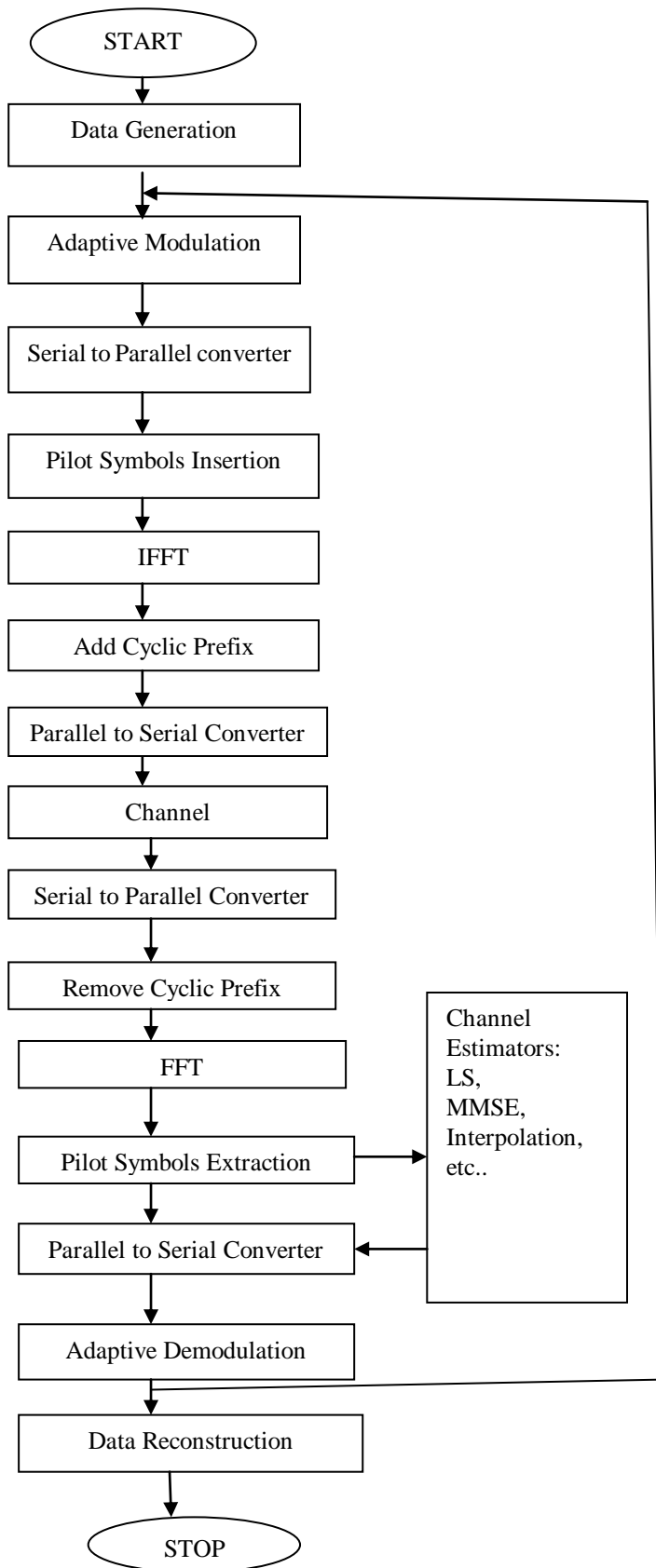


Figure II: Algorithm for Adaptive Modulation with Channel Estimation in OFDM

M-ary QAM) for least square and minimum mean square error channel estimation schemes are determined at target BER 10^{-2} and are listed in tables II,III,IV and V.

Table. I :Design System parameters

Parameter	Specifications
Number of bits	2048
Number of subcarriers	2048,1024,683,512,410,342, 293
IFFT/FFT size	256
Guard time duration	2
SNR range	0-33 dB
Modulation schemes	2, 4, 8, 16, 32, 64, 128
Pilot carriers ratio	1/8
Number of channel taps	2, 6, 10, 15
Channel model	AWGN

Table II: Threshold levels of modulation schemes (MPSK) for LS channel estimated OFDM system

Sl No:	Modulation	Threshold range
1	BPSK	$SNR \leq 7$
2	QPSK	$7.1 \leq SNR \leq 8$
3	8PSK	$8.1 \leq SNR \leq 16$
4	16PSK	$16.1 \leq SNR \leq 22$
5	32PSK	$22.1 \leq SNR \leq 25$
6	64PSK	$25.1 \leq SNR \leq 27$
7	128PSK	$27.1 \leq SNR \leq 33$

Table III: Threshold levels of modulation schemes (MQAM) for LS channel estimated OFDM system

Sl No:	Modulation	Threshold range (in dB)
1	4QAM	$SNR \leq 8$
2	8 QAM	$8.1 \leq SNR \leq 16$
3	16 QAM	$16.1 \leq SNR \leq 22$
4	32 QAM	$22.1 \leq SNR \leq 25$
5	64 QAM	$25.1 \leq SNR \leq 27$
6	128 QAM	$27.1 \leq SNR \leq 33$

Table IV: Threshold levels of modulation schemes (MPSK) for MMSE channel estimated OFDM system

Sl No:	Modulation	Threshold range
1	BPSK	$SNR \leq 7$
2	QPSK	$7.1 \leq SNR \leq 8$
3	8PSK	$8.1 \leq SNR \leq 16$
4	16PSK	$16.1 \leq SNR \leq 22$
5	32PSK	$22.1 \leq SNR \leq 25$
6	64PSK	$25.1 \leq SNR \leq 27$
7	128PSK	$27.1 \leq SNR \leq 33$

Table V: Threshold levels of modulation schemes (MQAM) for MMSE channel estimated OFDM system

Sl No:	Modulation	Threshold range (in dB)
1	4QAM	$SNR \leq 8$
2	8QAM	$8.1 \leq SNR \leq 16$
3	16QAM	$16.1 \leq SNR \leq 22$
4	32QAM	$22.1 \leq SNR \leq 25$
5	64QAM	$25.1 \leq SNR \leq 27$
6	128QAM	$27.1 \leq SNR \leq 33$

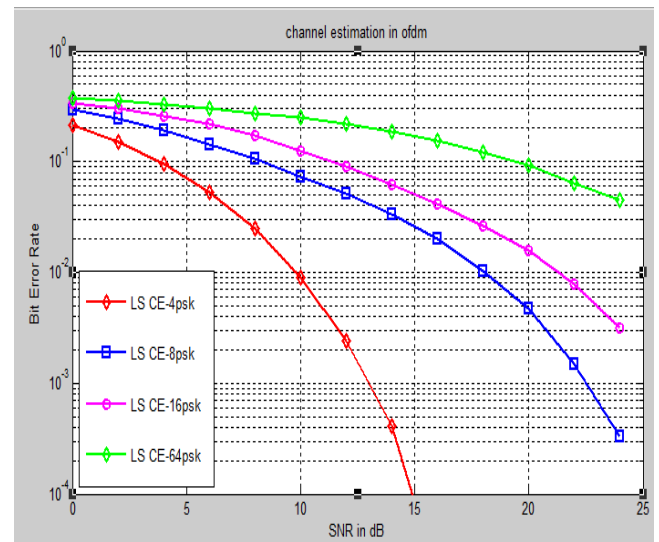


Figure III: BER performance of LS Channel estimated OFDM using M-ary PSK.

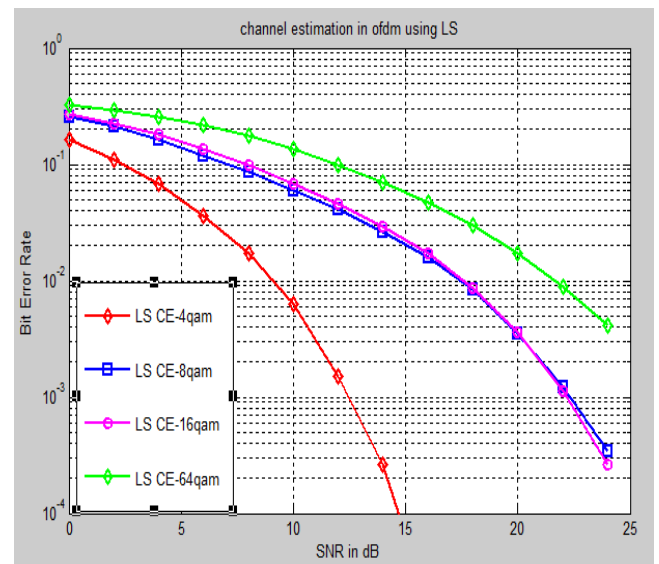


Figure IV: BER performance of LS Channel Estimated OFDM using M-ary QAM.

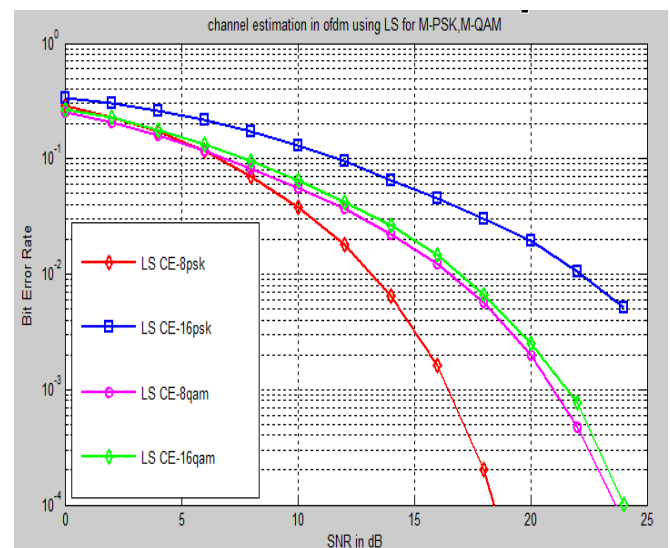


Figure V: BER performance comparison between M-ary PSK, and M-ary QAM for LS Channel Estimated OFDM.

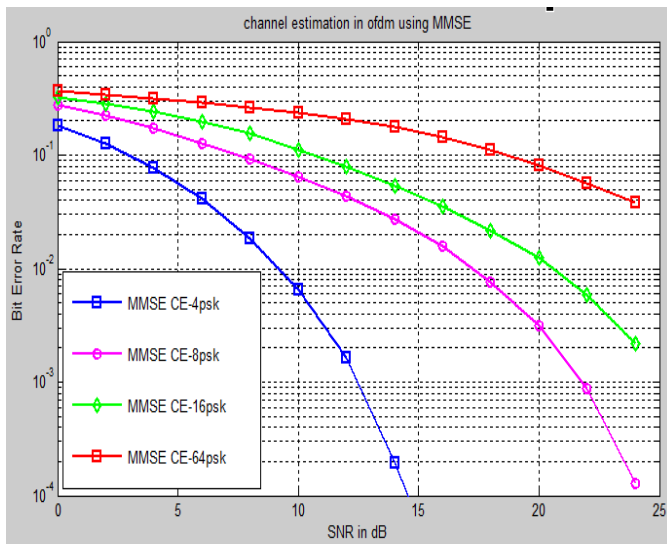


Figure VI: BER performance of MMSE Channel Estimated OFDM using M-PSK.

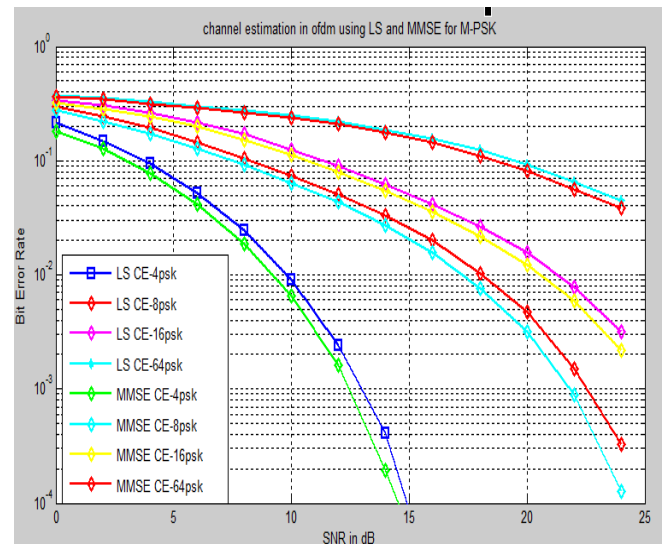


Figure IX: BER performance comparison of LS & MMSE Channel Estimation using M-PSK in OFDM system

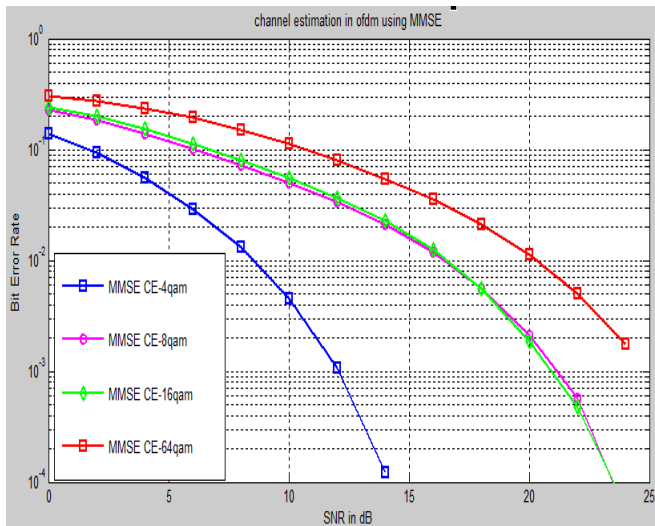


Figure VII: BER performance of MMSE Channel Estimated OFDM using M-QAM.

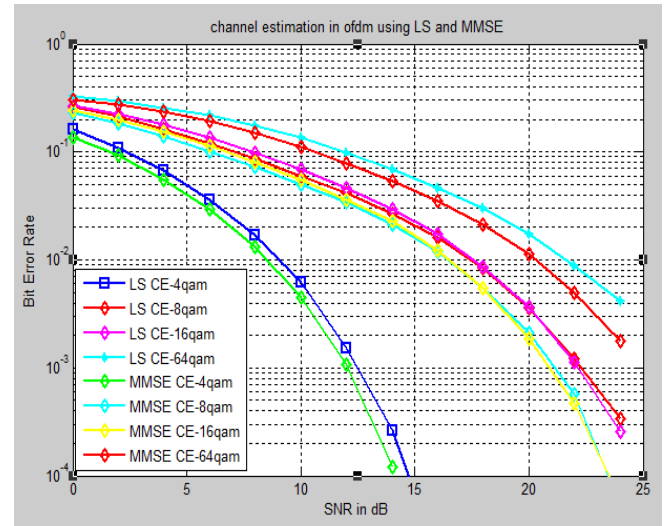


Figure X: BER performance of LS & MMSE Channel estimation using M-QAM in OFDM System

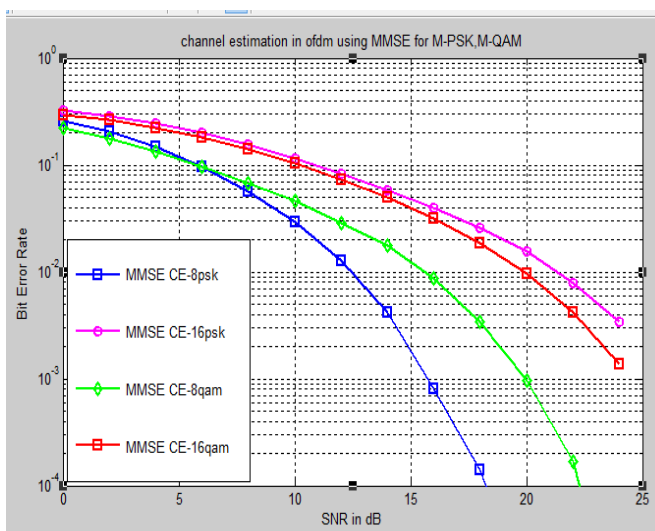


Figure VIII: BER performance of MMSE Channel estimated OFDM using M-PSK, M-QAM

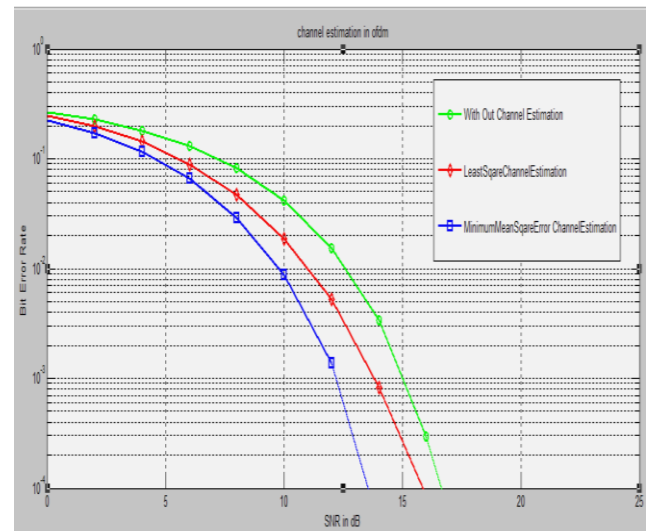


Figure XI: BER Performance of OFDM with and without channel estimation

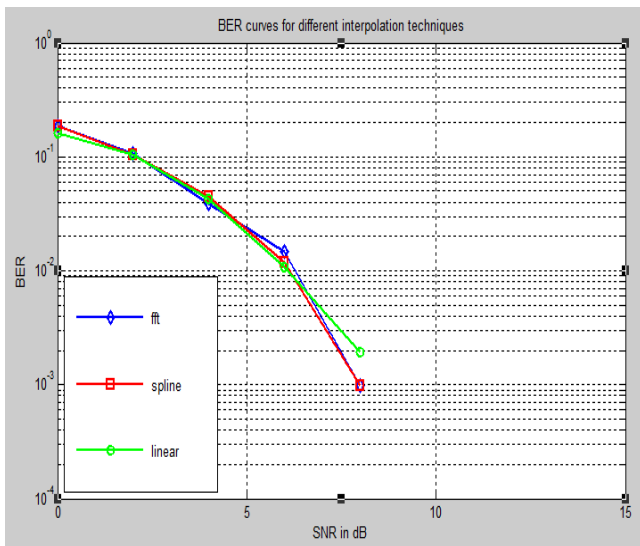


Figure XII: BER Performance of OFDM using Interpolation based Channel Estimation

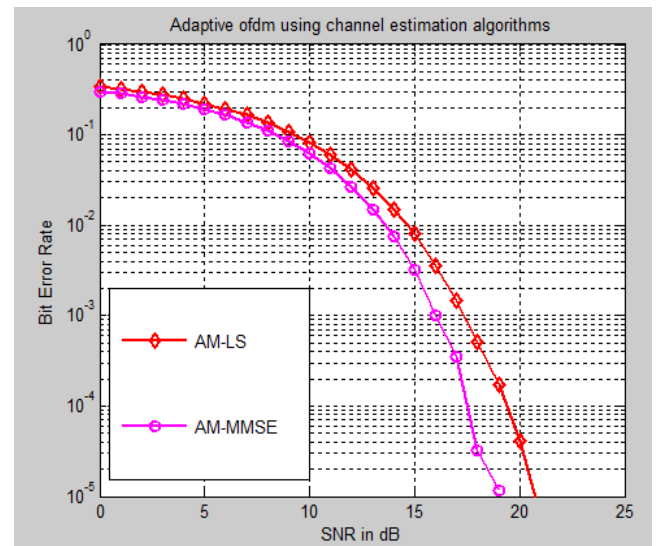


Figure XV: BER Performance comparison of OFDM using Adaptive Modulation with LS and MMSE Channel Estimation

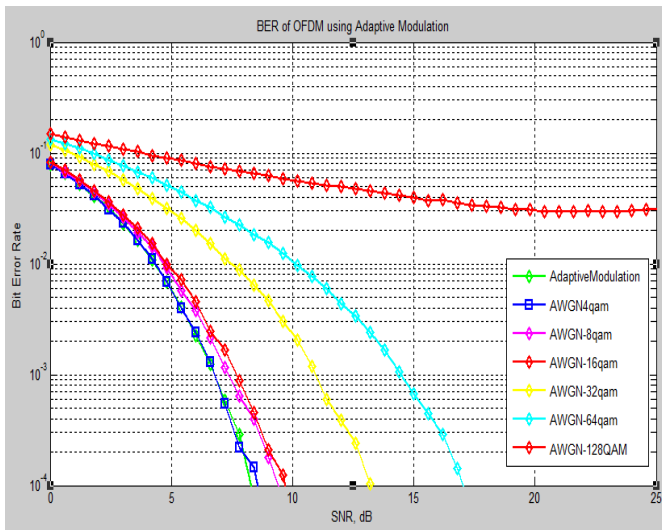


Figure XIII: BER Performance comparison of OFDM for Adaptive Modulation and various orders of Modulation

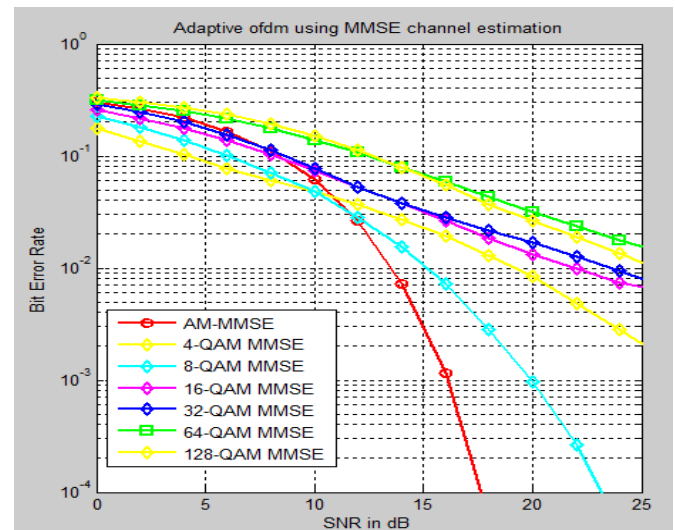


Figure XVI: BER Performance comparison between MMSE channel estimated Adaptive OFDM and MMSE channel estimated OFDM.

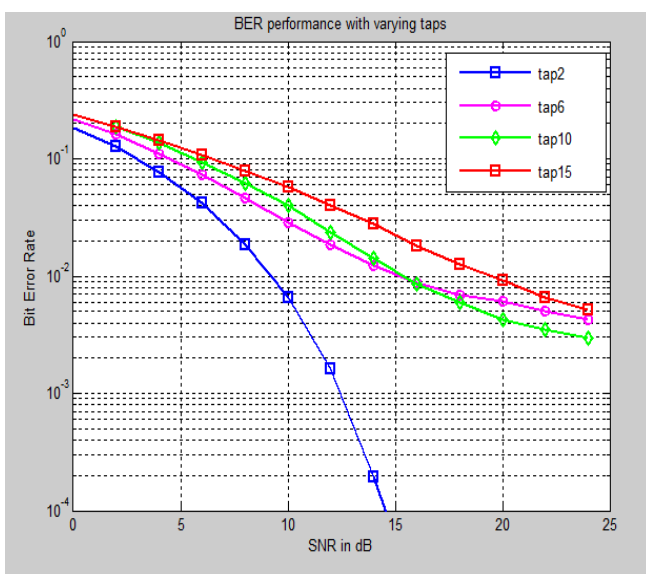


Figure XIV: BER Performance of OFDM in Multipath environment.

VII. CONCLUSION

In this work OFDM system is implemented with 512 subcarriers, digital modulator, multipath AWGN channel, and channel estimators. BER performance is analyzed for various digital modulation schemes, LS, MMSE channel estimations, adaptive modulation and combination of channel estimators and adaptive modulation

From the results it is concluded that BER performance degrades with increase in order of modulation, the performance of QAM is better over PSK for constant throughput. BER performance of MMSE is better over LS channel estimator and the BER Performance of Interpolation estimator is superior over LS and MMSE. The lower order modulation schemes result in better BER performance over the higher order modulation schemes at the cost of spectral efficiency and throughput. The BER performance of MMSE channel estimated adaptive OFDM is superior over individual channel estimated OFDM systems and adaptive OFDM system. Hence from the results finally it is concluded

that the proposed method improves OFDM system performance significantly.

REFERENCES

- [1] Sinem Coleri, Mustafa Ergen, Anuj Puri, Ahmad Bahai "Channel Estimation techniques based on Pilot arrangement in OFDM Systems," IEEE Transactions on broadcasting, vol. 48, No. 3, pp 223-229, September 2002.
- [2] Meng-Han Hsieh, and Che-Ho Wei, "Channel estimation for OFDM systems based on Comb type Pilot arrangement in frequency selective fading channels", IEEE transactions on consumer electronics, vol. 44, No. 1, February 1998.
- [3] Jihyung Kim, Jeongho Park and Daesix Hong, "Performance analysis of channel estimation in OFDM systems", IEEE signal processing letters vol. 12, No. 1, January 2005.
- [4] A.Z.M.TouhidulIslam and Indraneel Misra, "Performance of Wireless OFDM System with LS-Interpolation-Based Channel Estimation in Multipath Fading Channel," International Journal on Computational Sciences & Applications (IJCSA), vol. 2, No. 5, October 2012.
- [5] Dongxu Shen, Zhifeng Diao, Kai Kit Wong and Victor O. K Li "Analysis of pilot assisted channel estimation for OFDM systems with transmit diversity", IEEE transactions on broadcasting, vol. 52, No. 2, PP. 193-202, June 2006
- [6] J. Faezah, and K. Sabira, "Adaptive Modulation for OFDM Systems," International Journal of Communication Networks and Information Security (IJCNIS), vol. 1, No. 2, August 2009.
- [7] Vineetha Mahathai, K. Martin Sagayam, "Comparison And Analysis Of Channel Estimation Algorithms In OFDM Systems", International Journal of Scientific & Technology Research, vol. 2, Issue 3, March 2013.
- [8] Srishatansh Pathak and Himanshu Sharma, "Channel Estimation in OFDM Systems", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 3, March 2013.
- [9] Sajjad Ahmed Ghauri, Sheraz Alam, M. Farhan Sohail, Asad Ali, Faizan Saleem, "Implementation of OFDM and Channel Estimation using LS and MMSE estimators", International Journal of Computer and Electronics Research vol. 2, Issue 1, Feb. 2013.
- [10] John R. Barry, Edward A. Lee, David G Messerschmitt, "Digital Communications", 3rd Edition, Springer International 2005
- [11] Sonali. D. Sahu, A. B. Nandagaonkar, "OFDM Channel Estimation using an MMSE Estimator of a Comb-type System", International Journal of Advanced Computer Research, vol. 3 No. 2, Issue 10, June 2013.
- [12] Aida Zier and Ridha Bouallegue, "Channel Estimation Study For Block-Pilot Insertion in OFDM Systems under slowly time varying conditions", International Journal of Computer Networks & Communications (IJCNC) vol. 3, No. 6, November 2011.
- [13] Deepa, Saranjeet Singh, "An Adaptive approach to Switching Coded Modulation in OFDM System under AWGN Channel", International Journal for Scientific Research & Development (IJSRD), vol. 3, Issue 07, 2014.

JPEG IMAGE STEGANALYSIS USING MACHINE LEARNING

Rahul Ranjan

M.Tech – Information Security and Cyber Forensics
SRM University, Kattankulathur
Chennai-603203, India

Ms Kirthiga Devi T.

Assistant Professor
Department of Information Technology
SRM University, Kattankulathur
Chennai-603203, India

Abstract— The project deals with detection of steganography content. Steganography is the process of hiding the secret information within an ordinary message, pictures, audio or videos. To reveal such content is more important to avoid usage by criminals. This project applies an approach of supervised machine learning to detect the presence of steganographic content coded by programs like Steghide in the JPEG images.

Keywords—Steganography, Stego-images, Cover-images, Steganalysis.

I. INTRODUCTION

Steganography is the process of hiding the secret information within an ordinary message. Steganography applies to any type of the medium. The steganogram could be text, image, audio or video.

A frequently asked question is, Who needs steganalysis? Closely related is who is using steganography. Unfortunately, satisfactory answer to this is hard to find. A standard claim in the literature is that terrorist organizations uses steganography to plan their operations. This claim seems to be founded on a report in USA Today, where it claimed that Osama Bin Laden was using internet in an 'e-jihad' half a year before he become famous in September 2001 [11].

The major problem lies in determining whether file is a steganogram or not.

With the wide use and abundance of steganography tools on the internet, law enforcement authorities have concerns in the trafficking of illicit material through web page images, audio and other files. Methods of detecting hidden information and understanding the overall structure of this technology are crucial in uncovering these activities.

II. BACKGROUND

A. What is Steganography?

Steganography is the process of hiding the secret information within an ordinary message. Steganography applies to any type of medium. The steganogram could be text, images, audio file, video or anything else that the user might want to send to another.

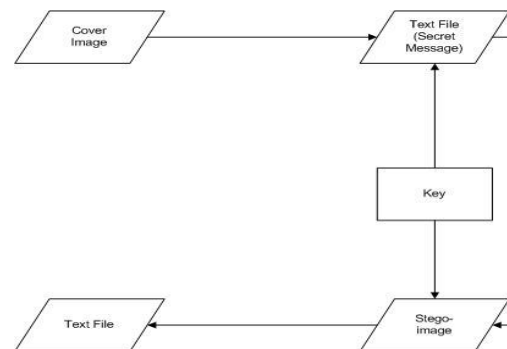


Figure 1: Process of Steganography

B. What is Steganalysis?

Steganalysis is the process of detecting the hidden content. A basic steganalyzer is an algorithm which takes a media file as input and outputs either steganogram or innocent. The message recovery is not the part of steganalysis [11].

C. Main Approaches to Steganalysis

We can distinguish between four known classes of image steganalysis. They are:

- Visual steganalysis
- Structural steganalysis
- Statistical steganalysis
- Learning Steganalysis

Visual Steganalysis is the most manual approach. In this full uncompressed images are inspected [11].

Structural Steganalysis looks for the give-away signs in the file format. A classic example is some of the software packages of the 1990's which inserted the name of the stego software in the comment field in the JPEG file [11].

Statistical Steganalysis uses methods from statistics to detect steganography and they require a statistical model, describing the probability distribution of steganograms and/or covers theoretically [11].

Learning Steganalysis overcomes the analytic challenge by obtaining a model through brute-force data analysis. The

solution comes from areas known as pattern recognition and machine learning [11].

Machine Learning

Learning is an aspect of intelligence, which is often defined as the ability to learn. In broad sense, machine learning is about extracting the information from data. In a standard data set this information is not readily available, so a lot of the work goes into looking for the right patterns in the data.

The task in steganalysis is to take an object and classify this into one of the two classes, either the class of steganograms or the class of clean images. This type of problem, of designing algorithm to map objects to a class is known as pattern recognition. In earlier days, pattern recognition was primarily based on statics and the approach was analytic. Machine learning provides an alternative to the analytic approach.

III. PROPOSED APPROACH

A. Creating Stego-images

The first step in the approach is to create stego-images from original images using the tool steghide.

Steghide is a steganography tool that is used to hide in various kind of image and audio files. The color- respectively sample frequencies are not changed thus making the embedding resistant against first-order statistical attack [14]. More can be found in [13].

B. Sample Extraction

The second step involves sample extraction, i.e, features that are extracted from both the original and stego images. The feature that can be extracted and be used to solve our problem is Huffman coding. To extract such kind of information from images a program JPEG Snoop [16] can be used.

JPEG Snoop can extract information such as:

- Quantization table matrix
- Chroma subsampling
- JPEG Quality
- Huffman's coding table
- EXIF metadata

Huffman's coding was designed by David Huffman in 1952. It has two properties - a code with a minimal length, it is not only the prefix code and is therefore uniquely decodable. The disadvantage is that we should know the probability distribution of the occurrence of each symbol. Sample Huffman's coding table of a clear and coded pictures are as follows (Table1 and Table 2)

Table 1: Huffman's Coding – Clear Picture

Bits	DC, Class0	DC, Class1	AC, Class0	AC, Class1
1	0	0	0	0
2	82	537	111597	41239
3	2811	494	39917	30606
4	886	602	46384	31571
5	837	542	30163	18650
6	724	475	5825	7639
7	547	293	14139	724
8	213	112	6943	3479
9	44	17	2526	842
10	0	0	2580	352
11	0	0	658	150
12	0	0	206	54
13	0	0	0	0
14	0	0	0	7
15	0	0	32	11
16	0	0	947	27

Table 2: Huffman's Coding – Coded Picture

Bits	DC, Class0	DC, Class1	AC, Class0	AC, Class1
1	0	0	0	0
2	240	534	111447	41366
3	2734	497	39851	30474
4	853	603	46280	31552
5	811	542	30122	18612
6	715	474	5796	7645
7	535	293	14067	716
8	212	112	6953	3524
9	44	17	2498	847
10	0	0	2569	357
11	0	0	621	158
12	0	0	179	54
13	0	0	0	0
14	0	0	0	7
15	0	0	15	11
16	0	0	681	28

C. Classifier

A decision tree classifier can be developed using scikit-learn [12] module of Python. A decision tree is flowchart like structure in which each internal node represents a “test” on attribute. The path from root to leaf represents classification rules. Decision Trees are a non-parametric supervised learning method used for classification and regression. The goal is to create a model that predicts the value of target variable by learning simple decision rules inferred from the data feature.

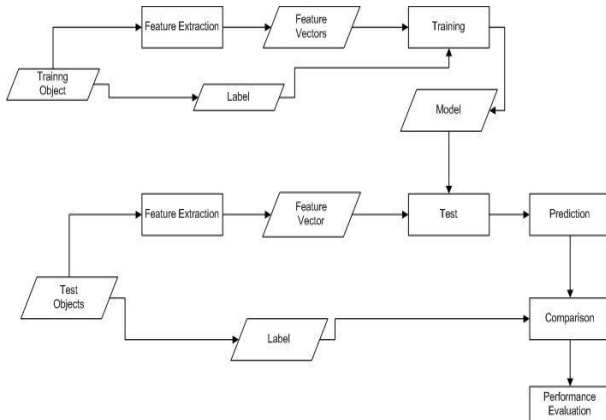


Figure 2: Learning Classifier

D. Training Sets

For training it is necessary to define suitable training sets. The authors used photos from ground truth image database [11]. In this group of photos a secret message will be inserted using the program steghide. The message is unique in every image due to a random generator of strings that will be used.

Huffman's coding data from JPEGSn00p will be transferred to training set-all four columns are to given line by line which will create a vector. Examples of clear and coded inputs in a training set are in Figure 3 and Figure 4.

{0,82,2811,886,837,724,547,213,44,0,0,0,0,0,0,0,537,494,
602,542,475,293,112,17,0,0,0,0,0,0,0,111597,38817,
46384,30163,5825,14139,6943,2526,2580,658,206,0,0,
32,947,0,41239,30606,31571,18650,7639,724,3479,842,
352,150,54,0,7,11,27}

Figure 3: Example of clear input in training set

{0,240,2734,853,811,715,535,212,44,0,0,0,0,0,0,0,534,49
7,603,542,474,293,112,17,0,0,0,0,0,0,0,111447,39851
,46280,30122,5796,14067,6953,2498,2569,621,179,0,0
15,681,0,41366,30474,31522,18612,7645,716,3524,847
,357,158,54,0,7,11,28}

Figure 4: Example of coded input in training set

As number show there is a difference but here are the examples of two pictures without and with secret messages inside (figure 5 and figure 6). For the first view there is no difference.



Figure 5: Picture without Secret Message (original image)



Figure 6: Picture with secret message (Stego Image)

IV. PROPOSED TOOL

A tool will be developed which will be using the classifier and model to predict the previously unseen images and classify the image as either a clean image or stego image.

The tool will first check whether the image is of JPEG image by verifying it with the magic number associated with JPEG format. If the image is verified, then the tool will classify the image using the model created by training sets.

The flow of the proposed tool is as follows:

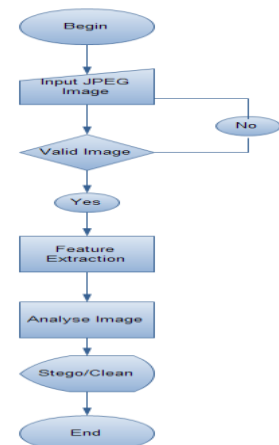


Figure 7: Flow chart of the tool

The proposed tool will be a GUI based tool which will take an image as an input, validate that it is a JPEG image file format

and then classify it in either a clean or stego image. The flow of the tool is described in figure 7. The tool will take an image as an input and first will verify the image is a JPEG image by verifying the magic number which is unique for every file format. If it is a valid JPEG image format, the tool will then extract the required features from the image and provide that data to the classifier. The classifier will try to predict the nature of image- clean or stego image- based on the trained model during the training phase of the project and at the end will display message according to the result. The tool will be developed in Python. The proposed screenshot of the tool are given in figure 8 and figure 9.

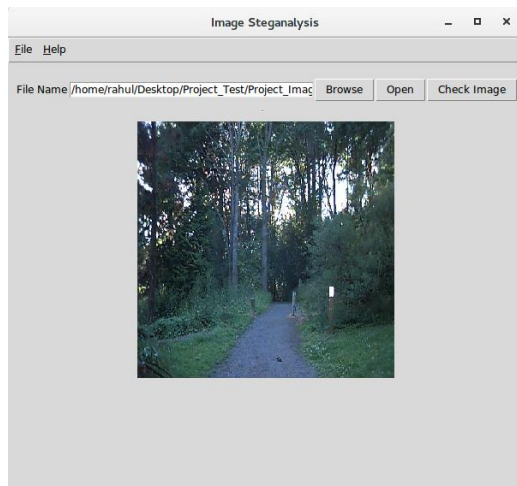


Figure 8: Proposed tool

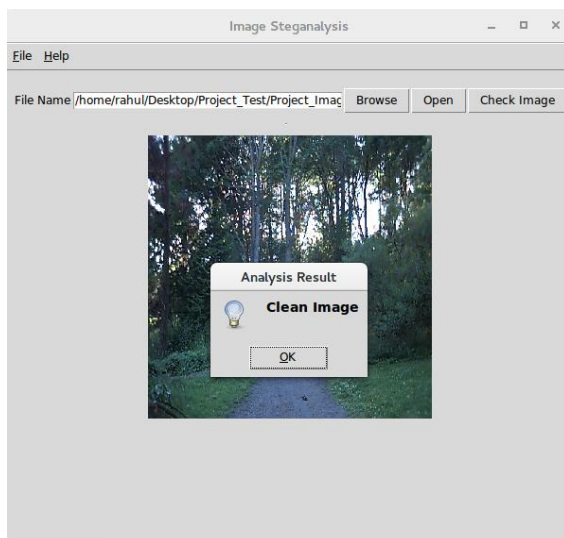


Figure 9: Proposed tool with result message

CONCLUSION

This paper dealt with an approach to detect steganographic content in images inserted by the program Steghide. It can be revealed with the use of Decision tree classifier.

Before detection of the clean or stego images was necessary to insert a message to some images firstly. For this coding purpose Steghide program was used. The further works proposes of creating a tool which will be using this classifier to classify the previously unseen images and also to learn to classify other formats of the images.

ACKNOWLEDGMENT

The research presented is being performed for the SRM University, Chennai, India in partial fulfillment of the requirements for the Master of Technology degree. I take this opportunity to express my profound gratitude and deep regards to my friends for their exemplary guidance, monitoring and constant encouragement. Prof S. Rajendran, for their patience and always being positive. I am thankful to all lecturers at SRM University for their support and comments.

REFERENCES

- [1] Masoud Nasorati, Roank Karimi, Mehdi Hariri, "An Introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011. 191-195 ISSN: 2222-2510
- [2] Andres Westfeld, "F5- A steganography algorithm", Technische Universit"at Dresden, Institute for System Architecture D-01062 Dresden, Germany westfeld@inf.tu-dresden.de
- [3] Catherine Holloway, "JPEG Image Compression: Transformation, Quantization and Encoding", Honours Linear Algebra, April 2008
- [4] Natarajan Meghanathan, Lopamudra Nayak, "STEGANALYSIS ALGORITHMS FOR DETECTING THE HIDDEN INFORMATION IN IMAGE, AUDIO AND VIDEO COVER MEDIA", International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010
- [5] Pedro Domingos, "A Few Useful Things to Know about Machine Learning", Department of Computer Science and Engineering University of Washington Seattle, WA 98195-2350, U.S.A. pedrod@cs.washington.edu
- [6] Fabian Pedregosa, Ga"el Varoquaux, Alexandre Gramfort, Vincent M"iche, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, Vincent Dubourg, David Cournapeau, "Scikit-learn: Machine Learning in Python", Journal of Machine Learning Research 12 (2011) 2825-2830 Submitted 3/11; Revised 8/11; Published 10/11
- [7] Mr. Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY", Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012
- [8] Andreas Grytting Furuseth, "Digital Forensics: Methods and tools for retrieval and analysis of security credentials and hidden data"
- [9] K Curran and K Bailey, "An evaluation of image-based steganography methods", International Journal of Digital Evidence, 2(2), 2003, www.ijde.org/docs/03 fall steganography.pdf Visited 1. Jun 2005.
- [10] Andreas Westfeld and Andreas Pfitzmann, "Attacks on Steganographic Systems Breaking the Steganographic utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned"
- [11] Schaathun, . "Steganography and Steganalysis", Machine Learning in Image Steganalysis, Schaathun/Machine Learning in Image Steganalysis, 2012
- [12] <http://imagedatabase.cs.washington.edu/groundtruth/>
- [13] <http://scikit-learn.org/stable/tutorial/basic/tutorial.html>
- [14] <http://steghide.sourceforge.net/>
- [15] <http://www.linuxlinks.com/article/20080504151119828/Steghide.html>
- [16] <http://www.impulseadventure.com/photo/jpeg-snoop.html>

Botnet: Switching c&c servers using RaspberryPI

Tejas B Waghela

M.Tech - Information Security & Cyber Forensics,
SRM University, Kattankulathur,
Chennai – 603203, Chennai, India

Ms. Krithiga Devi T

Assistant Professor,
SRM University, Kattankulathur,
Chennai – 603203, Chennai, India

Abstract— Challenges for detection of botnet for forensic investigation is crucial because new models of botnet using different techniques are emerging everyday by lurking attackers in a deep web. Locating c&c servers of a botnet through usual methods might be useful in some cases when there are defects in the architecture & its inner implementation of botnet. In this paper several possibilities of making a different types of botnet are discussed, which can make detection of botmaster and c&c servers complex when usual botnet detection methods are used. This gives opportunities to the security professionals to explore different botnet architectures, its operations, locating c&c (command and control) servers & botmaster. It will encourage security professional for finding new techniques for detection of botnet & find the procedure for dealing with the same. A combination of various techniques and approaches can develop a new type of botnet which contains different perspectives that makes detection and location of botmaster and c&c servers intricate, which will also break open paths for the white hats to fight on such cyber weapons.

Keywords—c&c servers, Botnet, TOR Proxy, Raspberry PI.

I. INTRODUCTION

In cyber security Botnet is one of the critical threat that should be handled by security professionals. Botnet is enrolled for malicious purposes like DDOS attack, cyber-espionage, spying, bitcoin mining etc. Antivirus providers are constantly reporting for this threat.

Botnet architecture can be characterized into basic three groups, centralized botnet [1], decentralized p2p (Peer to Peer) botnet [1] and TOR based botnet [2].

1. Centralized botnet:

A single command and control server manages the entire botnet and its operation. Because of its simple design & architecture, this type of botnet is very easy to implement and rule. Botmasters can easily handle all compromised computers. Drawback of centralized structure is single c&c server will lead to critical failure that will collapse the entire botnet if detected by security admin.

2. Decentralized p2p botnet:

In Decentralized p2p botnet the hurdle of centralized Botnet has been removed [3]. It contains multiple c&c servers.

To achieve resiliency, a complete distributed network and different types of protocols can be used to shelter detectability. These c&c servers can transfer information with each other and also commands to the zombie computers. So, any failure of one c&c server will not disturb whole botnet operations & its work flow.

3. TOR based botnet:

TOR stands for “The Onion Router”. TOR is a network which provides anonymity to the users. Encrypted traffic is routed from this network. It avoids traffic analysis and allows public services without revealing physical location. Standard design of the TOR is vulnerable too for some attacks, though one can use TOR with some precautions for being anonymous to some extent. TOR cannot be claimed for providing foolproof anonymity, but one can say it could provide good enough anonymity services. Using TOR, Web services can be implemented. It is called as, hidden services which are accessible via TOR software only. Tracing back of actual IP address and physical location from where operations are being conducted will be made difficult by using this software. Botmasters create c&c servers as a hidden service. It makes the task of locating these servers tricky for forensic investigator. But because of some limitations & vulnerabilities of TOR the location can be traced back, definitely it can consume some countable amount of time, thus making it convoluted. According to presentation given by Dannis Brown at DefCon18 [4] the idea of TOR based botnet was demonstrated a possible implementation of a c&c servers over TOR network to provide anonymity. Guarnieri has detected and analyzed the first Tor-based botnet in 2012 [5].

Rest of the paper is cataloged into BACKGROUND, describing bots, botnets, zombie PCs, c&c servers, TOR, Raspberry PI. Section III PROPOSED APPROACH pens down different botnet architectures that consist of various elements and which concentrate on hardening of traceability that enhances thinking of the ethical security geeks like an attacker at different levels in the architecture. Malicious software, c&c servers and raspberry PI are core elements of proposed structure. Later sections of the paper composes of CONCLUSION, ACKNOWLEDGEMENT and REFERENCES.

II. BACKGROUND

This section explains the working of bots, c&c servers, TOR, TOR proxies and raspberry PI.

A. Bot and Zombie pc

The term Bot was derived from “roBot”. This contains some sort of scripts that are good in repetitive tasks. Attacker writes malicious code or virus to infect a computer for dishonorable purposes. After malicious infections computer becomes a bot and it allows attacker to take a full control over it. These computers sometimes referred as a Zombie & group of computers are called as zombie army which are key elements for botnet.

B. Botnet

The botnet is an overlay network of all compromised computers that are controlled by a botmaster. Malware takes care to connect it further with c&c servers and other zombie computers.

C. Command and Control Servers (c&c servers).

C&C servers are centralized computers that issues commands to the zombies and which revert back to the c&c servers. Attacker tries to keep size of those commands minimal. C&C servers are very crucial in botnets.

D. Proxy, Proxy Chaining and TOR.

Proxy servers are gateways which resides in between your computer and the destination webpage. All traffic is routed from your computer to the web proxy and vice versa. One can use multiple proxies from source to destination. When multiple proxies are used and traffic is routed from multiple proxy servers it is called proxy chaining. Rather using proxy servers, one can also use a TOR network. This stratagem will help to get anonymity.

E. Raspberry PI.

Raspberry Pi is a low cost, credit-card sized computer that when attached to a computer monitor or TV, uses a standard keyboard and mouse. It is a small computer device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python [6].

III. PROPOSED APPROACH

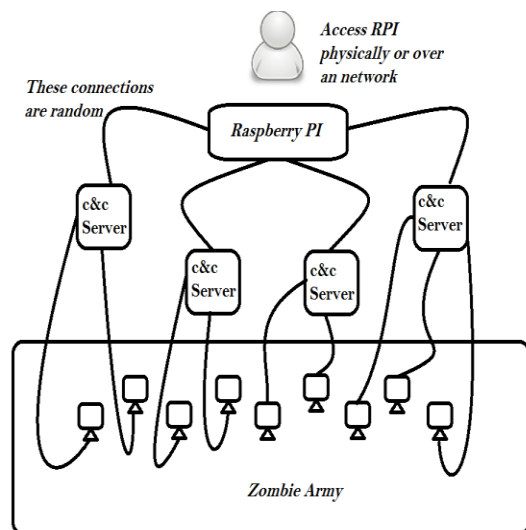


Figure No 01: Proposed architecture of botnet using Raspberry PI

In the above figure a model of Botnet with some modifications is proposed. Architecture is divided into three modules. Each module can have a multiple ways of implementation. One can take either choices or combination of them, from each module. The modules are categorized, namely,

1. Zombie Army
2. Domain Fluxing
3. Switching C&C Servers using Raspberry PI

A. Module 1: Zombie Army

Key element for creating a zombie army is the malware. Attacker will create an extremely powerful malware for creating Botnet army. Attacker will be more concentrating on malware's resiliency, infecting factor or its spreading power, polymorphism, stealthiness, its signature, encryptions etc. Some malwares die and are reborn with new capabilities and modifications of its inner working or replace itself with newer version. These malwares are responsible for creating backdoor, connecting to command and control server (request-response) & converting a clean computer into a zombie.

After creating a dedicated malware for Botnet, process connects zombie pc to the c&c server. If this connection is simple then it's easy to trace back to the c&c server. So attacker will make all transactions for minimal amount of time and try to make it as anonymous as possible. Basically there are two possible ways to do it.

1. Through Proxy
2. Using TOR

1. Using Proxy Servers:

Proxy and proxy chaining methods are used to make connections using a gateway between source &

destination. The source will become a zombie pc and destination will be the c&c servers. All these proxy servers should be mandatorily embedded within a malware and attacker has to make sure all these proxy servers are persistent. Generally these proxy servers are situated at remote places from each other. So if security admin wants to locate proxy servers and wants to contact admin or owner of proxy server, obviously it will take prolonged time to deal & give results. Secondly, attacker can route packets from multiple ways, this completely depends on the functioning of the malware. For an example, malware contains some set of proxy servers, one function can choose random proxy servers & creates proxy chain from the set of proxies available. It will also confirms that availability of this route for particular time period and make transaction to the c&c server. For next command transactions it will ensures that packets will not choose the same route because of random proxy selection algorithm. Attacker always ensures about minimal time for each transactions of commands between c&c server and zombie army to avoid pattern recognition, thus clearing his tracks.

Disadvantage:

- If proxy server is not persistent, the connection between zombie PC and c&c server will break.

2. Using TOR :

At DefCon18, Dannis Brown presented, possible implementation of c&c sever in a TOR network. C&C servers can be hidden in a TOR services. Guarnieri[5] has analyzed and detected first implemented TOR-based botnet. All communication made between TOR and Zombies using TOR hidden services & TOR Network. TOR is having its own capabilities to provide anonymity up to some extent, using that botmasters can harden the botnet detection. There can be possible number of .onion pseudo-domain where c&c servers are hosted, attackers make sure that domains are live for a particular time period only.

Algorithm for establishing connection using TOR

Step 1: All pseudo random domains of .onion hidden services are embedded within a malware.
Step 2: Malware functions ensures which domain is available for this time.
Step 3: After locating valid web server (.onion pseudo domain accessible using TOR only), it will open a predefined port for accepting commands from available c&c server which is hosted as a hidden service of TOR.
Step 4: Now zombies are able to receive & executes command.

Disadvantage:

- Vulnerabilities of TOR needs to take in to consideration.
- Vulnerable to sink hole attacks [7].

Both ways to connect zombie army to the c&c servers are having their own limitations and risk of detectability.

So security admins should focus on both scenarios. If any zombie pc found then security admins has to find the root malware. Next will have to perform reverse engineering of a malware. Generally reverse engineering of any program takes quite time, so it is possible that within a these timeline c&c servers become inactive or can be dead.

B. Module 2: Domain fluxing

The scheme of domain fluxing is hiding Command & Control servers in a long list of IP addresses. Generally Domain generation algorithm (DGA) are used for this. Domain Generation Algorithm is a program that creates variant number of a given domain name. Using DGA, botmasters learns to hide their command and control servers. Inclusion of DGA is optional for this architecture, because it is fully depends on a botmaster. New techniques are emerging everyday so DGA is quite an old technique but it is still used. Various DGA detection techniques are also available [8].

If TOR based botnet is used then within a malware attacker tries to embed mechanism of creating TOR hidden services in a zombie computer on defined port. By default nothing is listening on defined port but when bot operator issues some command using any IRC channel then malware will activate proxy on that port. Once this is done, bot can easily contact any .onion website from the list of pseudo-random domains which are hardcoded in a malware to establish a connection.

Covert channels are very important for creating such complex architecture.

C. Module 3: Switching c&c servers using Raspberry PI

A bot herder or a botmaster can control zombie army usually by means of different communication channels. The most common example is IRC botnet. Command-and-control takes place using IRC server running on public IRC network. A bot runs their hidden services and plays around. Generally bot herder makes his own private protocols which uses internet and produce successful results for client-server architecture. These protocols and programs has to be embedded in a malware. Communication between Server programs, Client programs and Protocols takes place over a network in form of encryption for its stealth and getting protection against detection from intrusion mechanism.

Command and control servers are usually made up by three ways.

1. Using IRC
2. Using LAMP Software bundle
3. Using API of a social networking websites (use of covert channels)

As stated previously IRC can be used to communicate with bots. But corporate environment will block all IRC communication using private network. Also firewall, antivirus, IDS, IPS, Honeypots and other botnet detection methods can detect and block the communication and takes further actions for bot herder and its operations. Basically c&c server architecture using IRC, HTTP [9] or using LAMP software bundle is so common. So, we can expect new and innovative type of client-server communication covert channels.

JPEG images, PDF files, Microsoft office Suits etc. can be used for covert channel communication in botnet. The most interesting covert channel is social networking websites. Sometimes networking sites like LinkedIn, twitter accounts are used for sending commands to the bots. These social networking sites are allowed in some corporate environments. These social networking sites do allow usage of their APIs for various purposes. As an example Twitter API allows to write status portion of the profile. Now, that status portion can be used for sending commands & retrieving reports from compromised computers [10].

Combination of all three modules are essence of proposed architecture. This is quite challenging for security admins to deal with such situations.

In this proposal Raspberry PI can be used to manage command and control servers. Raspberry PI can be used for administration and management of c&c servers. One central device will control all the c&c servers. This device is capable of selecting a particular one c&c for specific amount of time. After that timespan Raspberry PI will select a different c&c server. Depending upon management & administration capabilities of Raspberry PI one can configure number of c&c for a single PI.

Either combinations of different c&c server's architectures can be used or covert channels for either set of c&c servers can be implemented. Raspberry PI, is portable and can be operated from anywhere. Attacker may use this device in public open Wi-Fi network zone to target victims. Attacker can automate this device using their programming skills & using self-executable program for replacing the c&c servers. Depending on configuration, attacker can manipulate the forensic investigator and collect data from c&c servers.

Each of the above three modules has its own objectives and limitations, as discussed in individual module.

Raspberry PI may prove a catastrophic device if used for an offensive purpose. Initially it was made for a school kids to better understand and learning purpose of programs and computers, but it soon became a constant tool used by black hats as hacking devices. Switching c&c servers on raspberry PI gives advantage to an attacker. This structure can be used for small task which can cause huge disruption.

IV. CONCLUSION

Getting resiliency and protecting failure of botnet by any kind of dirty play is the mindset of the bot herder. In each of the module we saw different variations & techniques employed now a days by an attackers. Possibly there are other techniques also adopted by an attacker but that possible information are made hidden to the public. Providing security & protecting infrastructure from any kind of available cyber weapons is necessary for the white hats.

Administering & handling c&c servers using Raspberry PI is the key proposal here. Raspberry PI is a amazing device which is made for learning basic programming and automations to the kids. Raspberry PI is capable of doing anything that normal computers can do. This could be game changing for all next upcoming technologies in future like IOT. Controlling c&c servers using Raspberry PI shows its power in destructive phase. Locating such device is also difficult. All positive and negative aspects to be considered for any innovative idea. Hackers are using such devices for negative purposes.

This paper provides necessary information & possible techniques that can motivate security admins to enhance botnet detection methods & mechanism. Hackers thinks that all techniques & ideas having their own drawbacks, failure points & vulnerability, Ethical hackers also should think same like a bad guys to overcome their destructives ideas and provide more security, enhancing available techniques and be prepared to protect IT infrastructure on any cost.

ACKNOWLEDGEMENT

The research presented is being performed for the SRM University in partial fulfillment of the requirements for the Master of Technology degree in Information Security & Cyber Forensics, at the SRM University, Chennai, India. I take this opportunity to express my gratitude to the Mr. Geogen George of IT Department for their encouragement, Prof S. Rajendran, for his guidance and all lecturers at SRM University for their support and comments.

REFERENCES

- [1] N.S.Raghava,V Divya Sahgal, Seema Chandna, "Classification of Botnet Detection Based on Botnet Architecture", 2012 International Conference on Communication Systems and Network Technologies International Conference, pp 569 572, 10.1109/CSNT.2012.128, IEEE
- [2] Matteo Casenove , Armando Miraglia , "Botnet over Tor: The illusion of hiding" , Cyber Conflict (CyCon 2014) 2014 6th International Conference, pp 273-282, 10.1109/CYCON.2014.691640

- [3] Avadhoot Joshi, Prof. M. S. Chaudhary, "Study of P2P Botnet", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. IV (Jul – Aug. 2014), pp 35-42
- [4] D. Brown, Resilient Botnet Command and Control with Tor, DefCon 18, 2010
- [5] Claudio Guarnieri, Mark Schloesser, Skynet, a Tor-powered botnet straight from Reddit, <https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit> , 03-Dec-2012
- [6] Raspberry PI, <https://www.raspberrypi.org/>
- [7] David Sancho and Rainer Link, Trend Micro Senior Threat Researchers, SINKHOLING BOTNETS, A Trend Micro Technical Paper
- [8] DGA, Infosec Institute, <http://resources.infosecinstitute.com/domain-generation-algorithm-dga/>
- [9] Esraa Alomari, Selvakumar Manickam, B. B. Gupta, Parminder Singh, Mohammed Anbar, Design, Deployment and use of HTTP-based Botnet (HBB) Testbed, ISBN-978-89-968650-3-2, pp 1265-1269
- [10] Jeremiah Talamantes, RedTeam Security Botnet Command and Control via Covert Channels, <http://www.redteamsecure.com/labs/post/28/Botnet-Command-and-Control-via-Covert-Channels>
- [11] GreAT - Kaspersky Lab's Global Research & Analysis Team, Full Analysis of Flame's Command & Control servers – Securelist; <https://securelist.com/blog/incidents/34216/full-analysis-of-flames-command-control-servers-27/>
- [12] Meng-Han Tsai, Kai-Chi Chang, Chang-Cheng Lin, Ching-Hao Mao, Huey-Ming Lee , " C&C Tracer: Botnet Command and Control Behavior Tracing", 978-1-4577-0653-0/11/\$26.00 ©2011 IEEE, pp 1859-1864
- [13] Sheharbano Khattak, Naurin Rasheed Ramay, Kamran Riaz Khan, Affan A. Syed, and Syed Ali Khayam, "A Taxonomy of Botnet Behavior, Detection, and Defense", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 2, pp 898-924, SECOND QUARTER 2014
- [14] Craig A. Schiller, Jim Binkley, David Harley, Gadi Evron, Tony Bradley, Carsten Willems, Michael Cross; ISBN-10: 1-59749-135-7; Botnet The Killer Web Apps; Syngress

Classification of Efficient Symmetric Key Cryptography Algorithms

Shivlal Mewada

Dept. of Computer Science,
MGCGV, Chitrakoot, Satna- India

Pradeep Sharma

Dept. of Computer Science,
Govt. Holkar Sc.College, Indore- India

S. S. Gautam

Dept. of Computer Science,
MGCGV, Chitrakoot, Satna- India

Abstract—Security threats have been a major concern as a result of emergence of technology in every aspect including internet market, computational and communication technologies. To solve this issue effective mechanism of “cryptography” is used to ensure integrity, privacy, availability, authentication, computability, identification and accuracy. Cryptology techniques like PKC and SKC are used of data recovery. In current work, we describe classification of efficient approach of symmetric cryptosystem architecture on the basis of attributes: effectiveness, scalability, flexibility, reliability and degree of security issues essential for safe wired and wireless communication. The work explores efficient private key algorithm based on security of individual system and scalability under criteria of memory-cpu utilization together with encryption performance. The investigation results in Rijndael algorithm as superior over other symmetric algorithm. The work opens a novel direction over cloud information security and internet of things.

Keywords— *Private key (Symmetric Cryptosystem SKC); Public Key (Asymmetric Cryptosystem PKC); wired communication; Wireless Communication; Variable key size and length (VKS/L).*

I. INTRODUCTION

Using recent cryptography techniques, security engineering exploits different mathematical techniques related to control access, authentication, authorization, data integrity, confidentiality aspects. it governs tools of security protocols and applicability in recent technology. The science of encipherment enriches cryptographic products, stimulated for ATM cards, e-mail, e-banking, e-trading, e-commerce and electronic signatures for secure communication and transaction. Conventionally Enciphering process transforms plain text to the scrambled cipher text [1,2,].

Cryptography technology can be divided as Symmetric key cryptography (SKC) algorithm and Asymmetric key Cryptography (AKC) algorithm.

In SKC encipherment or secret key encipherment, only 1-key is used to enciphering and deciphering information or data. In SKC keys, two keys are used; one private and another public keys. Public key is used for encipherment and private key is used for decipherment. Public key encipherment is based on mathematical functions,

computationally intensive. There are many popular and well-respected symmetric cryptography algorithms like; DES, triple-DES, Blowfish, CAST, Serpent, TEA , AES (Rijndael) , Twofish, IDEA, RC-6, and MARS.

AKC algorithms also known as public key encipherment is a form of crypto system in which encipherment and decipherment are modern encipherment technology mathematically performed using various keys like; public key and private key. Public key is used for encipherment and private key is used for decipherment. There are many popular and well-respected asymmetric cryptography algorithms like; RSA, Diffie-Hellman keys and Digital Signatures etc.

Referring to figure-1,2 & 3, elucidation can be made obvious that enciphering can be done in variety of ways described below:

- *Secret Key Cryptography*: Utilizes only one key for both transformation and recovery.
- *Public Key Cryptography (PKC)*: Utilizes one key for transformation and another for recovery.
- *Hash or digest Entity*: Utilizes an non-invertible mathematical transformation "encrypt" information.

Private-key cryptography commonly uses algorithms likes: DES, RC2, RC4, RC5, RC6, Blowfish, Advanced Encryption Standard (Rijndael) [2,3,4,5], etc.

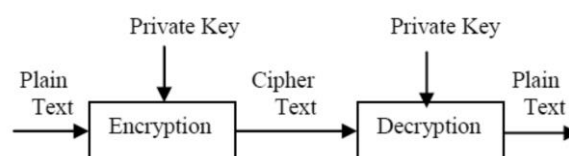


Figure 1. Private-key cryptography

Public-key cryptography Alice uses to encrypt-key that is distributed publically for transformation of plain text and only the authorized person with dedicated-private can decrypt the cipher text through his own private key. Private Key used secretly uses algorithms likes: RSA, Diffie-Hellman keys, SSH, digital signature, knapsack algorithm, SSL [2,3,4,5], etc.

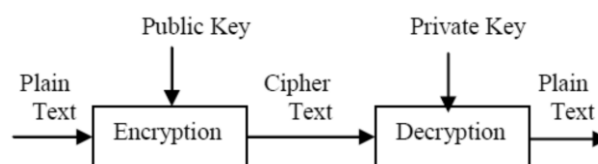


Figure 2. Public-key cryptography

Corresponding Author : Shivlal Mewada,
Department of Computer Science, MGCGV, Chitrakoot- India
e-mail: shivlal.mewada.1986@ieee.org

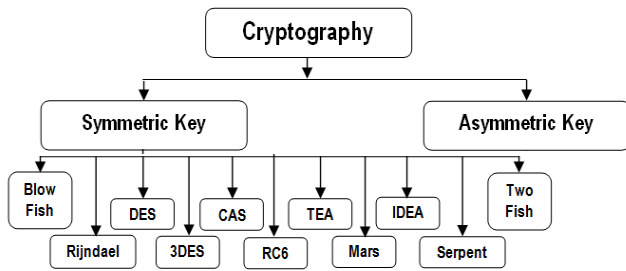


Figure 3. Classification of some SKC Algorithms

This study describes an overview and evaluation of different SKC algorithms namely; DES, triple-DES, Blowfish, CAST5, Serpent, TEA, AES (Rijndael), Twofish, IDEA, RC-6, and MARS.

The work explores efficient private key algorithm based on security of individual system and scalability under criteria of memory-cpu utilization together with encryption performance.

Rest of the paper is organized as follows, Section I contains the introduction of crypto system and symmetric algorithms, Section II contain the related work of symmetric algorithm, Section III contain the basic parameters/attributes for symmetric algorithms, Section IV contain the architecture SKC algorithms, Section V contain the Security aspects of SKC Algorithms, Section VI contain Scalability feature of SKC algorithms, VII contain the flexibility of SKC algorithms, VIII contain the limitations of different SKC Algorithms, IX contain the Comparative Explorations of efficient SKC algorithms, Section X contain the recommendation of AES algorithm and Section XI concludes research work with future directions.

II. RELATED WORK

This section traces the history backward on timeline of security methods[1,2,3] In Two fish was found better using web based tool crypter over alternative symmetric versions and attempt to identify parameters; like- throughput, CPU-Memory consumption and utilization, energy consumption[5,6], attacks, encryption-decryption time. In [2,6] the comparison of three private algorithms like; DES, Triple DES, and Blowfish on processing time and concluded that key generation time for all these DES, Triple DES, and Blowfish algorithms is almost same but there is a difference in time taken by CPU for encryption, SunOS Blowfish found > DES > Triple DES. Analysis of CPU time for producing secret key, transformation and recovery time. In [7] for input image file, AES took less-encryption and decryption-time than DES. In [2,8] the author compared DES, AES, Blowfish for ECB, CBC, CFB, OFB mode on different file sizes varying from 3kb to 203kb. Blowfish yield better performance for all block cipher modes tested and OFB mode gives good performance than other modes. In [2,9] AES, DES, 3-DES and Blowfish with twofish for varying file size and compared the encrypt time on various computing machines. The author concluded that speed of Blowfish algorithm > DES algorithm > Triple DES algorithm and CFB takes more time than ECB cipher block mode. Apart from these traditional symmetric algorithms AVK

approach is taking shape in the direction of time variant key, That believes in frequently changing key instead of extending key size for security enhancement. Apart from developing cryptosystem has to investigated under various tools and mining approaches for identifying weakness[9,10,11,12].

III. SKC ALGORITHMS

In this section, *private-key cryptography* algorithms will be chosen for specific application to analyse positive(supportive) and negative aspects, based on attributes like; architecture; security; limitations; scalability; flexibility, different existing algorithm can be evaluated.

A. Parameter

Architecture: To investigate structure, function and operations influencing execution and features and implemented. Use of encryption and decryption cryptosystem like SKC and PKC determines whether algorithm is private or not.

Security: Strength of cryptic algorithm with attribute of key size for encoding. Stronger the encryption implies longer keys, measured in bit.

Flexibility: It is the ability of algorithm to support modifications as per the requirements of cryptosystems.

Scalability: It supports Memory Utilisation, Encryption rate, S/W & H/W performance; Computational efficiency.

Limitations: It is susceptibility to different types of attacks.

B. Evaluation Methodology

Selective evaluation mechanism is needed to cater the demand of a particular system, with greater deficiencies with peer algorithms. Scalability of different algorithms has been claimed by the authors of those algorithms and on the basis of scalability of different algorithms their simulations were carried out [10,11,12].

IV. ARCHITECTURE OF SKC ALGORITHMS

Data Encryption Standard [13]: The DES is private-key cryptography extends spine concept of Feistel Structure (Substitution-Permutation Network) accepts a 64 bit input with 16 iterations + a keysize (56 or 128 bits). Initially 64 bits (blocks size), but in every byte 1 bit as 'parity'. A single plain text block transformed into cipher text over the different stages.

Triple Data Encryption Standard: TDES performs 3 iterations of DES with 3-different keys. For 64 bit plain text with 16x3 rounds + length of Key 168-bits+ permutation into 16 sub- keys(48- bit length) + 8 substitution boxes in reverse order for decryption [8].

Blowfish Algorithm: It includes key-expansion and data-transformation part with 64 bit input text + 16 iteration, key length up to 448 bits, 18 sub- keys each of 32- bit length can be used on 32 or 64-bit processors[14, 15].

International Data Encryption Algorithm: With 64 bit input text + 8 iterations + keysize 128-bit permuted into 52 sub-keys size 128-bits. [6].

Tiny Encryption Algorithm: With 64 bit i/p text + 64 iteration + key 128-bit with non uniform 32 cycles TEA provides improved security [16].

CAST : With 64 bit input + 12 to 16 rounds + keysize from 40 -128-bit key, using 4 s-boxes it works for both encryption/decryption [9].

Advanced Encryption Standard (Rijndael): With block sizes 128, 192 and 256 bits., key size - 128,192 and 256 bits. It depends on the length of key e.g. 10 round for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. In AES, plain text transformed into cipher text after passing through the different stages like. byte substitution, row shift, column and round key.

RC-6: It is a Feistel Structured SKC algorithm that makes use of a 128 bit input text with 20 iterations and a variable key size (VKS) of 128/192/256 bits. As RC6 is based on RC algorithm, can accommodate huge variation of word-

size/key-length/ no of rounds, RC-6 utilizes S- boxes and thus same symmetric algorithm can be applied inversely for decipherment.

Serpent: It is a SKC algorithm that is based on hierarchical arrangement of substitution-Box (S) and permutation-box(P). It consists of a 128 bit input plain text with 32 cycles and a VKL of 128/192/256 bits. It also contains eight s- boxes and same algorithm is used in reversed for decipherment.

Twofish: This SKC algorithm is based on the Feistel Structure. The Rijndael is a block cipher that uses a 128 bit input text with 16 iterations and a VKL of 128/192/256 bit. It makes use of four substitution- boxes (depending on Key) and same algorithm is used in reversed for decipherment.

MARS: It is SKC algorithm based on heterogeneous Structure that make use of a 128 bit input text with 32 iterations and a VKL from 128- 448 bits (multiple of 32-bit). It only contains a single substitution - box the same algorithm is used in reversed for decipherment. All these are presented in table 1.

TABLE 1. SKC ALGORITHMS ARCHITECTURE

Algorithm	Algo_Structure	Input Text (Plain/ Cipher)	Key Size (Max/Min)	Cipher Type	Substitution S-Box	Number of Iterations
DES	Feistel cipher network	64 bits	56	Block cipher	8	16
T-DES	Feistel cipher network	64 bits	168	Block cipher	8	48
Blowfish	Feistel cipher network	64 bits	128-448	Block cipher	4	16
IDEA	S-Permutation network	64 bits	128	Block cipher	-	8
TEA	Feistel cipher network	64 bits	128	Block cipher	-	64 (32 Cycles)
CAST	Feistel cipher network	64 bits	40-128	Block cipher	4	12-16
AES	Feistel cipher network	128 Bits	128,192,256	Block cipher	1	10,12,14
RC6	Festial structure	128 Bits	128,192,256	Block cipher	N/A	20
Serpent	Festial structure	128 Bits	128,192,,256	Block cipher	8	32
Twofish	Festial	128 Bits	128,192,256	Block cipher	4	16
MARS	Festial	128 Bits	128-448	Block cipher	1	32

V. SECURITY OF SKC ALGORITHMS

Data Encryption Standard: It uses 56 bit key size (7.2×10^{16} permutations), it reduces the risk of unauthorized computation or acquisition. Further with little changes in the input text, encrypted text changes significantly. The backward compatibility, and cost of upgrading, feature point out the risk of exposure.

Triple Data Encryption Standard: Triple DES use a larger size of key (168-bits > 112 bits of DES) to encrypt. reduces meet-in-the-middle possibility [17, 18] and provides high level of security in comparison and evaluation.

Blowfish: With Key size (128-448 bits) and independent key in each round, makes system invulnerable and and complicated. Thus autonomy is more highly enviable.

International Data Encryption Algorithm: With 128 bit key size it increases security. Nobody has encountered any algebraic or linear attacks in this SKC algorithm. Attackers

directly approaches on even keys, so that it can break IDEA reduced to six rounds [18].

Tiny Encryption Algorithm: With 128 bit key size it structures and simply secure implementation.

CAST: With VKS operation and function to enhance cast security strength, the security of CAST is resistant against both linear, differential attacks.

Advanced Encryption Standard: With VKS upto 256-bit, it renders all attacks impractical. An implicit assumption is that the attacker has access to the computational fastest supercomputers. The attacks include differential and linear cryptanalysis. With extra h-w and slightly degraded performance, it mask out timing, power and other side channels attacks.

RC-6: RC-6 security lies in the completely random series of its output bits with 15 iterations or less, running on input blocks of 128 bits, one of the attributes to make an

encipherment algorithm resistant against the attacks due to random bit series. A linear cryptanalysis attack can be launched for 16 iterations RC-6, but requires 2^{119} known input texts, which make the feasibility of such attack impossible. The RC6 algorithm is also resistant towards differential cipher analysis (greater than 12 rounds).

Serpent- It is based on more conventional security approaches than the other Rijndael finalists, opting a larger security margin. According to the author of serpent 16 iterations serpent quite adequate against all known types of attack, but as an indemnity against future discoveries in cryptanalysis it is extended to 32 iterations. In order to avoid the collision attack Serpent usually discredits to modify keys well before 264 blocks have been encrypted. Serpent with its minimum potential (only half number of iterations) is still as secure as that of three-key triple DES.

Twofish- This SKC is robust and highly strong against associated-key attacks even with slide attack and the related key differential attack. With no weak keys it can be used to launch any related key attack.

MARS- MARS has enhanced security and faster than 3-DES/DES. It gives an iterated cipher with unusually 32 rounds. The middle cycles of MARS are its powerful component. The security of MARS is dependent on the set {data-rotations, functions with Boolean complexity}. So,

Visual Cryptanalysis is hard for MARS. MARS algorithm is highly resistant to attack sets = {Relative-key-attacks, Differential-attacks, timing attacks}.

VI. SCALABILITY OF SKC ALGORITHMS

In this section, we explain of scalability of various private key SKC algorithms, and these SKC algorithms are examined depending upon encryption performance and memory utilization through key scheduling.

The SKC memory utilization will be for efficiency and performance. Encryption rate should be as small as possible. The hw/sw compatibility should match with SKC Algorithm for better performance.

The figure-4 displays memory utilization and encryption performance of various algorithms. In [19,20] algorithm speed has been analyzed on a variety of general hw/sw platforms. Figure-4 shows performance analysis on the set = {memory utilization, encryption performance, hw/sw implementation}.

So, we compare eleven symmetric cryptography algorithms the graphs provide in figure-4. AES algorithm performance for very good and optimum memory utilization.

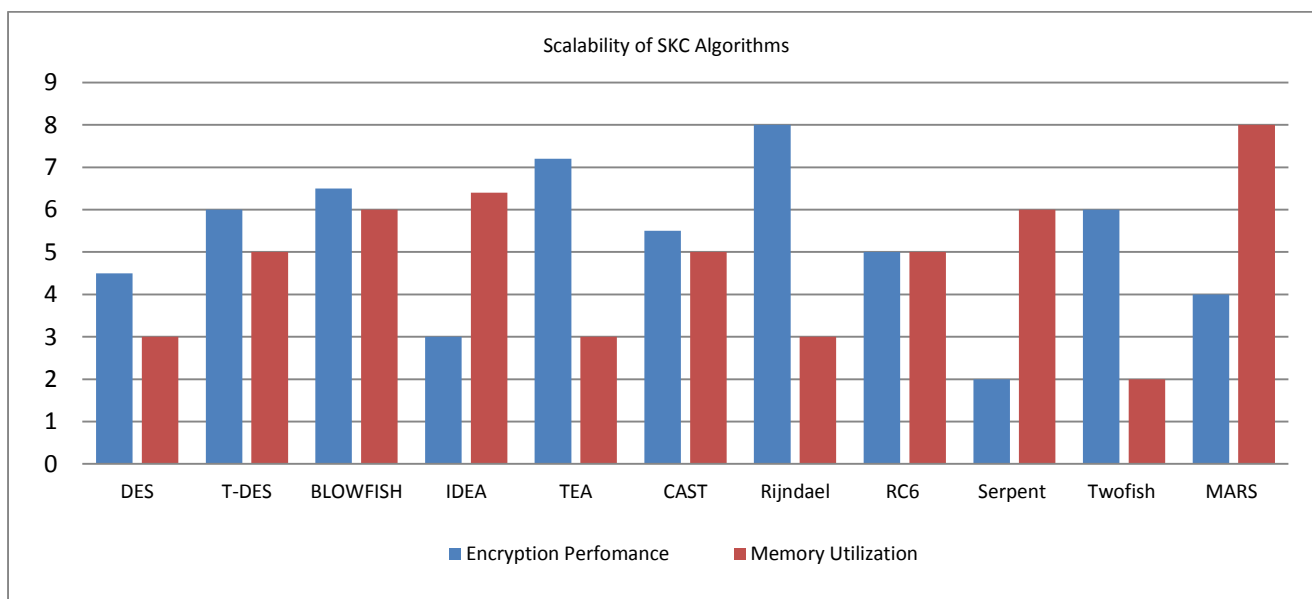


Figure 4. Scalability: Memory Utilization and Encryption Performance

VII. FLEXIBILITY OF SKC ALGORITHMS

In this section, we explain of flexibility of SKC towards modifications flexibility.

TABLE 2. SUMMARY OF PRIVATE ALGORITHMS FLEXIBILITY

Algorithms	Flexibility	Modification	Remarks
DES	No	None	Feistel Structure (DES) does not support any changes
T-DES	Yes	168	Feistel Structure (TDES) with varied key size extended to 168 bits
Blowfish	Yes	64- 448	The key length must be divisible by 32bit.
IDEA	No	None	Feistel Structure (IDEA) does not support any changes

TEA	No	None	Feistel Structure (TEA) does not support any changes
CAST	Yes	64,128,256	64 bits cast is flexible network modified to 128-256 bits, increased security and strength.
AES (Rijndael)	Yes	128,192,256	Rijndael algorithm was extendable multiple 64 bits, key size
RC6	Yes	128-2048	It has a VKL and can be extended to 2048 bits however the VKL must be a multiple of 32 bits
Serpent	Yes	256	It's keys are always padded to 256 bits. The padding consists of a "1" bit followed by "0" bits.
Twofish	Yes	256	It's keys, other than the default sizes, are always padded with "0" bits up to the next default
MARS	Yes	128-448	It's operates with VKL, but the key length must be multiples of 32 bits

VIII. LIMITATIONS OF SKC ALGORITHMS

Data Encryption Standard: prone to systematic attacks.

Triple Data Encryption Standard: T-DES is used in differential and related-key attacks and meet-in-the-middle attack.

Blowfish: With weak keys in 4 rounds it is exposed to differential attacks with large no. of weak keys.

International Data Encryption Algorithm: weak keys selection will lead to following vulnerabilities {Collision attack, key-schedule attacks ,correlated-key, differential timing attacks}.

Tiny Encryption Algorithm: with minimum of 126 bits related key attack involving 223 chosen plain texts under a related-key pair, with a complexity of 232 it is slow.

CAST: It is susceptible to differential related-key attack., 217 chosen plaintexts , related-key query .

Rijndael: With observed mathematical and statistical property it is vulnerable to attack.

RC-6: In RC-6, for a single class of weak keys, it is observed that full arbitrariness is not achieved for up to 17 iterations of the algorithm. No other limitations were identified.

Serpent: No such limitation was found in serpent; however the 32 iterations make Serpent a bit slower and complex to implement on small blocks.

Twofish: It is sensitive to chosen-key attacks that affect reduction in security, when applied to hash function.

MARS: No significant limitations is seen in MARS. Due to involvement of variety of component involved in MARS. the simple iteration function of MARS are relatively complex to analyze and making implementation of MARS on hardware is a bit difficult and complex.

IX. COMPARATIVE EXPLORATIONS OF SKC ALGORITHMS

Rijndael is secure, safe, faster and better, Still it has flaws in such as weak keys, insecure transmission of secret keys,

speed, control access, flexibility, integrity, authentication, authorization and reliability .the algorithm is suited to implementation in hardware. data encryption standard = IDEA w.r.t. speed., so 3DES is poor performance. In Blow Fish weak key attacks its three-round vision, slowed in speed but much faster than DES and international data encryption algorithm.

X. RECOMMENDATION

Security cannot be reliable if data transmission is not secure including security risks to information as hackers are always to steal critical information for better performance if advanced encryption standard cryptic algorithm factors are considered accurately. All the recommendations mentioned above would help improve security, scalability, integrity, control access, authentication, encryption-performance (high) and memory-utilization (minimum) of the cloud computing system.

XI. CONCLUSION

Encryption algorithm plays very important role in communication security, cloud security and information security. In this work, the analysis of private block algorithms based on chosen matrices. The objective is to analyze the performance of the most popular SKC algorithms for security, cryptic-flexibility, authentication, reliability, robustness, scalability for limitation of SKC algorithms. It's strength and weakness for application. During this reseaserch work it was observed that AES is the best SKC in accordance with security, flexibility, encryption performance and memory utilization. According to our findings alternative SKC algorithms also wich are competent but AES algorithms found to be the best in terms of encryption performance and memory utilization.

FUTURE WROK

Recently in literature alternative symmetric cryptosystem are being developed, Automatic Variable Key based cryptosystem [2,3,12] is one such approach.The impact of latest advanes of neural network, Genetic algorithm, Swarm intelligence is also influencing the cryptosystem design.The influence of these algorithm in IOT, Cloud infrastructures and machine to machine communication has to be tested for AES and DES scalability.

REFERENCES

- [1]. Krishna Kumar Pandey, Vikas Rangari, Sitiesh Kumar Sinha, “ An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security”, *International Journal of Computer Applications*, Volume 74– No. 20, pp(29-33) July 2013
- [2]. Shaligram Prajapat, at. al., “Sparse approach for realizing AVK for Symmetric Key Encryption”, *International Journal of Recent Development in Engineering and Technology*, Volume 2, Special Issue 4, pp(15-18) June 2014.
- [3]. Prajapat, S. , Rajput, D., Thakur, R.S., “Time variant approach towards symmetric key”, Published by IEEE: Science and Information Conference (SAI-13), , pp(398- 405), 7-9 Oct. 2013.
- [4]. G.A.V.Rama Chandra Rao, P.V.Lakshmi, and N.Ravi Shankar, A New Modular Multiplication Method in Public Key Cryptosystem”, *International Journal of Network Security*, Vol.15, No.1, pp(23-27), Jan. 2013.
- [5]. Hanno Scharwaechter et. al., “Heinrich Meyr ASIP Architecture Exploration for Efficient Ipsec Encryption: A Case Study”, 8th International Workshop, SCOPES-2004, Amsterdam, The Netherlands, pp (33-46) September 2-3, 2004.
- [6]. James Neuchâtel at. al., “Report on the Development of the Advanced Encryption Standard (AES)”, *Journal of Research of the National Institute of Standards and Technology*, Volume 106, Number 3, May–June, pp(511–577) 2001.
- [7]. Kamahi, N.A at. al., “Performance evaluation of three Encryption/Decryption Algorithms”, *IEEE 46th Midwest Symposium on Circuits and Systems*, Vol. 2, Issue 1, 30 pp. (790-793), Dec. 2003, DOI:10.1109/MWSCAS.2003.1562405, Print ISBN: 0-7803-8294-3
- [8]. S. Sony, H. Agrawal, M. Sharma, “Analysis and comparison between AES and DES Cryptographic Algorithm”, *International Journal of Engineering and Innovative Technology*, Vol. 2, Issue 6, pp(362-365), December 2012.
- [9]. J. Taker and N. Kumar, “DES, AES and Blowfish: Private Key Cryptography Algorithms Simulation Based Performance Analysis”, *International Journal of Emerging Technology and Advanced Engineering*, Vol. 1, Issue 2, , pp.(6-12). December 2011.
- [10]. Aamer Nadeem, Dr M. Younus Javed, “A Performance Comparison of Data Encryption Algorithms”, *IEEE-First International Conference on Information and Communication Technologies (ICICT)*, pp 84-89 27-28 Aug. 2005, DOI: 10.1109/ICICT.2005.1598556, Print ISBN: 0-7803-9421-6
- [11]. Meyer, C.H., “Cryptography-a state of the art review”, *IEEE-CompEuro '89.*, 'VLSI and Computer Peripherals. VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks, pp (150-154), 8-12 May 1989. DOI:10.1109/CMPEUR.1989.93462
- [12]. Shaligram Prajapat, Ramjeevan Singh Thakur, “ Various Approaches towards Cryptanalysis”, *International Journal of Computer Applications (0975 – 8887) Volume 127 – No.14*, pp(15-24), October 2015.
- [13]. Dadhich, A.; Gupta, A.; Yadav, S., “Swarm Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm”, *IEEE:International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp: (378 – 383), 7-8 Feb. 2014, DOI: 10.1109/ICICT.2014.6781312
- [14]. Alabaichi, A., Ahmad, F., Mahmood, R., “Security analysis of blowfish algorithm”, *IEEE: 2nd International Conference on Informatics and Applications (ICIA-13)*, 23-25 Sept. 2013, pp(12 - 18), DOI: 10.1109/ICoIA.2013.6650222, Print ISBN:978-1-4673-5255-0
- [15]. Tingyuan Nie, Teng Zhang, “A study of DES and Blowfish encryption algorithm”, *IEEE Region 10 Conference*, pp(1-4), 23-26 Jan. 2009, DOI:10.1109/TENCON.2009.5396115, E-ISBN: 978-1-4244-4547-9
- [16]. Manisha Yadav, Mauli Joshi, Akshita, “Improved Secure Data Transfer Using Tiny Encryption Algorithm and Video Steganography”, *International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 12*, pp. 547-550, December 2013.
- [17]. Verma, O.P., Agarwal, R., Dafouti, D., Tyagi, S., “Performance analysis of data encryption algorithms”, *IEEE: International Conference on Electronics Computer Technology (ICECT)*, pp:399 – 403, 8-10 April 2011
- [18]. Zibideh, W.Y.; Matalgah, M.M., “Energy consumptions analysis for a class of symmetric encryption algorithm”, *IEEE: Radio and Wireless Symposium (RWS)*, pp: 268 - 270, 19-23 Jan. 2014, DOI: 10.1109/RWS.2014.6830130
- [19]. Ayushi, “A Symmetric Key Cryptographic Algorithm”, *International Journal of Computer Applications Volume 1 – No. 15*, pp (1-4). 2010.
- [20]. Fiskiran, A.M.; Lee, R.B., “Performance Impact of Addressing Modes on Encryption Algorithms”, *IEEE: International Conference on Computer Design (ICCD 2001)*, pp (542 - 545), 23-26 Sep 2001, Print ISBN: 0-7695-1200-3 , DOI:10.1109/ICCD.2001.955088

Age Estimation Framework Based On Geometric & Appearance Feature-Based Methods

Rania Salah El-Sayed
Department of Computer science
Faculty of Science
Al-Azhar University
Cairo. Egypt

ABSTRACT—Age estimation has become increasingly important, due to the fact it has a variety of potentially useful applications, such as forensic art, electronic consumer relationship management, security control and surveillance, cosmetology, entertainment and biometrics. In this paper we propose framework for age estimation. It's provides new insights into issue of feature extraction. We use the hybrid features, which are a combination of global and local features; Global features are obtained with Active Appearance Models (AAM). Local features are extracted with applying multiple Gabor filters to extract wrinkle feature each of which is designed based on the regional direction of the wrinkles, and then apply a local binary pattern (LBP), capable of extracting the detailed textures of skin. We conduct extensive experiments on standard Age estimation (FG-Net) database to verify the performance of proposed method. And we compare the result with other approach.

Keywords: Age estimation, local binary pattern (LBP), Active Appearance Models (AAM), Gabor filter, support vector machine (SVM), support vector regression (SVR).

1. INTRODUCTION

Human age estimation is one of the most challenging problems in computer vision and pattern recognition. Because of its important applications in age-based image retrieval [1], internet access control, security control and surveillance, biometrics [2], human-computer interaction (HCI), and electronic customer relationship management (ECRM)[3].

In such applications, various feature can be estimated from a detect face image to further system reactions. For example, if the user's age is estimated by a computer, an age specific human computer interaction (ASHCI) system may be developed for

secure network/system access control. The ASHCI system ensures young kids have no access to internet pages with adult materials. A vending machine, secured by the ASHCI system, can refuse to sell alcohol or cigarettes to the underage people [4].

The task of automatically recognizing different age in human-computer environment is significant and challenging. A variety of systems have been developed to perform human age estimation and each system consists of three stages:[5] first, face detection; second, feature extraction then facial classification. Age estimation system can be represent as figure 1.

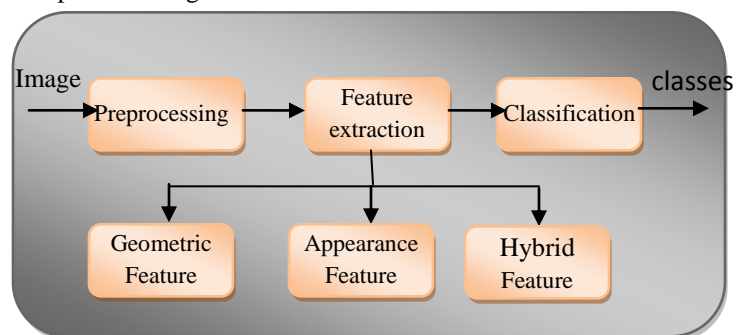


Figure 1 Age estimation system

Feature extraction is very important in age estimation, since the extracted features greatly affect the classification performance. So we effort has been directed towards the extraction of discriminative aging features. These features can be categorized into local and global features, and hybrid features, which are a combination of the global and local features.

There are some main categories [6,7] that can categorize most existing image-based age estimation methods, such as Anthropometric models[8,10],

Based on the measurements and proportions of the human faces. Active appearance models, Based on the statistical face model AAM[13,14] proposed by T. Cootes et al. Aging pattern subspace[11], Based on the AGES method proposed by Geng et al. Age manifold, Based on the manifold[4] embedding techniques to learn the low- dimensional aging trend. Appearance feature models, Based on aging-related features extracted from face images.

The last step of an automatic age estimation system is classification and regression. Most classification methods applied to age estimation are Nearest neighbor, Multilayer perception, Self-organizing map (SOM), age group classification, SVM, and neural network classifier.

In regression use Semi-Definite Programming (SDP) to solve the regression problem. Multiple linear regression. Support vector regression (SVR)[12,16].

In this research we propose a framework which can achieve age estimation, by using hybrid feature based methods that apply AAM [14] then extract Wrinkle feature by Gabor filter set considering regional direction of wrinkles and extract Skin feature by using local binary pattern method (LBP)[5,15] after feature extracted we start in classification phase using SVM and SVR.

This paper is organized as follows. Section 1 is this introduction. Section 2 discusses relevant related works from the literature. In section 3, active appearance model will be discussed. Local binary pattern discuss in section 4. Section 5, details of proposed algorithm are presented. Section 6, provides the details of the conducted experiments along with results .The paper concludes with a brief summary of results and proposal of future research directions in section 7.

2. RELATED WORK

Different researchers have used different approaches to estimate the human ages. Some systems concentrate in two stages: feature extraction and expression classification. Asuman Günay and Vasif V. Nabyev extract feature Based on AAM and 2D-DCT Features of Facial Images then applying regression [20].

Sung Eun Choi et al. estimated age using a hierarchical classifier based on global and local facial features[5].

Lanitis et al. [18] used the active appearance models (AAMs) by combining shape and appearance facial features. Age estimation was treated as a classification problem and solved by the shortest distance classifier and neural networks.

Jianyi Liu et al.[19] used fuzzy age label first, and then merged into the Support Vector Regression (SVR).

Takimoto et al. [23] used both the Sobel filter and the Gabor jet in order to distinguish a deep wrinkle from a fine wrinkle.

Jun-DaXia and Chung-Lin Huang [21] proposed an age classification method using wrinkle features extracted by the Sobel filter along with the hair color features.

Baddrud Z. Laskar et al. use Artificial Neural Networks and Gene Expression Programming based age estimation using facial features [22].

Wei-Lun Chao et al. combine distance metric learning and dimensionality reduction to better explore the connections between facial features and age labels. Then, exploit the intrinsic ordinal relationship among human ages [24].

Ranjan Jana et al.[26] estimate the real age of a human by analyzing wrinkle area of face images. Wrinkle geography areas are detected and wrinkle features are extracted from face image. Depend on wrinkle features, each face image is clustered using fuzzy c-means clustering algorithm.

In this paper we introduce new hybrid system based on AAM for geometric feature , Gabor wavelet filter & LBP for appearance feature and in classification phase we use classifier SVM and regression (SVR) to estimate age. Experimental results show how these techniques reduce error rate of age estimation.

3. ACTIVE APPEARANCE MODELS

The active appearance model (AAM)[14] is used to estimate age as geometric features in this paper.

AAM is a computer vision algorithm for matching a statistical model of object shape and appearance to a new image. They are built during a training phase. A set of images, together with coordinates of landmarks that appear in all of the images, is provided to the training supervisor [27].

AAM Models using the principal component analysis (PCA), and is able to generate various instances using only a small number of parameters [25,28]. Therefore, an AAM has been widely used for face modeling and facial feature point extraction. In order to construct the shape model, i points were selected in the facial images to compose a facial shape

$$X = [x_i : x_i \in \mathbb{R}^D]_{i=1}^n \quad (1)$$

The mean shape is produced with taking the mean of the landmark points in the training set as

$$\bar{X} = \frac{1}{n} \sum_{i=1}^n X_i \quad (2)$$

PCA is applied to the data to extract the main principal components along which the training set varies from the mean shape. If the total scatter matrix S is defined as [29]

$$S = \sum_{i=1}^n (x_i - \bar{x})(x_i - \bar{x})^T \quad (3)$$

Any training set of images can be approximated by

$$X = \bar{X} + P_s b_s \quad (4)$$

Where \bar{X} is the mean shape, P_s is a set of orthogonal principal modes of variation and b_s is a set of shape parameters.

For facial shape s , 68 landmark points on each face image were utilized in this paper, as shown in Fig. 2, therefore $i=68$. For the test data, the 68 landmark points can be manually obtained by human or automatically obtained by an AAM fitting.

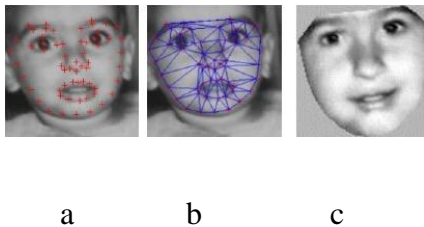


Figure 2. a) face image labeled with 68 landmark points b) Result of the Delaunay triangulation used in warping process c) face normalization

4. LOCAL BINARY PATTERN

The local binary pattern operator is an image operator which transforms an image into an array or image of integer labels describing small-scale appearance of the image [30]. These labels or their statistics, most commonly the histogram, are then used for further image analysis. The basic local binary pattern operator, introduced by Ojala et al. [31], was based on the assumption that texture has locally two complementary aspects, a pattern and its strength.

The original LBP operator labels the pixel of the image by comparing it with the surrounding pixels in its 3×3 -neighbourhood as [5] illustrated in fig 3.

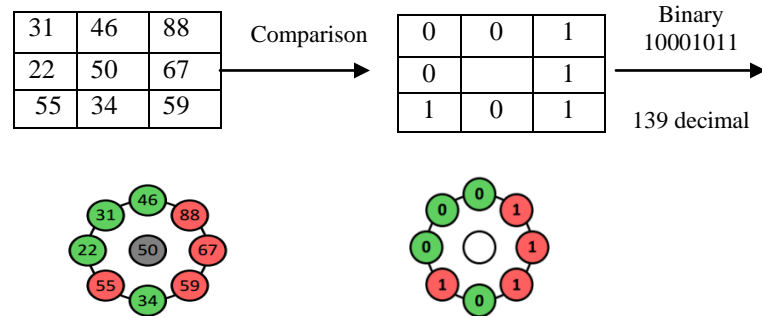


Figure 3: The original LBP operator

The generic local binary pattern operator is derived from this joint distribution. As in the case of basic LBP, it is obtained by summing the thresholded differences weighted by powers of two. The $LBP_{P,R}$ operator is defined as [15]

$$LBP(x_c, y_c) = \sum_{n=0}^{P-1} s(i_n - i_c) 2^n \quad (5)$$

where i_c corresponds to the gray value of the center pixel (x_c, y_c) , in to the gray value of the 8 surrounding pixels, and function $s(x)$ is defined as:

$$s(x) = \begin{cases} 1 & \text{if } x \geq 0 \\ 0 & \text{if } x < 0 \end{cases} \quad (6)$$

5. PROPOSED FRAMEWORK

Our proposed framework for age estimation works in four steps. First, we apply AAM [6] to extract geometric feature from image. In the geometric features-based systems, the shape and locations of major facial components such as mouth, nose, eyes, and brows, are detected in the images.

Our approaches used in such system are Active Appearance Model (AAM) [5], manually locating a number of facial points. Second, we normalized image and apply multiple Gabor wavelet filter.

The Gabor wavelet representation of images allows description of spatial frequency structure in the image while preserving information about spatial relations.

Let $r(x,y)$ be the original image $f(x,y)$ convolved with a 2D Gabor function $g(x,y)$ [7]

$$r(x,y) = f(x,y) * g(x,y)$$

where $*$ denotes the convolution operator and with $g(x,y)$ being a 2D Gabor filter. figure4 show gabor filter after apply on image.

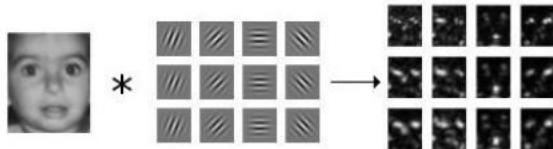


Figure 4. Convolution of the face image with the Gabor filter

the face image is convolved with multi-scale and multi-orientation Gabor filters first. Then third, the LBP operator is applied to each pixel of the Gabor magnitude images as illustrated in Figure 5.

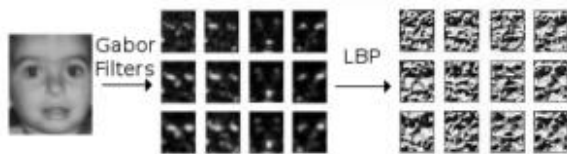


Figure 5. LBP operator after apply multiple Gabor filter

And then we fusion the geometric (AAM) & appearance feature (GW+ LBP) and fourth is the last step classification using SVM then regression using SVR to estimate age. The system architecture is shown in Figure 6. We focus in this paper on the procedures for feature extraction.

6. EXPERIMENTS

The proposed algorithm for age estimation is divided into two steps. First the facial landmarks for

the face image are detected automatically using AAM[6,32]. Then image is cropped to area covering a fixed number of points generated from the AAM step. Secondly, we used detected face as input to filtered by a set of Gabor functions. The filtered outputs undergo LBP to small-scale appearance of the image. Then we fusion two output and classify it with SVM then undergo to regression processes to select specific age as shown in figure 6.

In this section, we quantitatively verify the performance of different age estimation systems. Using FG-NET Aging Database [32] is used to train and test the proposed method. This database contains 1,002 face images from 82 subjects with approximately 10 images per subject. The ages in the database are distributed in a wide range from 0 to 69. Figure 7 show Example different ages images from FG-NET database. Images in the database display facial appearance changes in pose, illumination, expression, etc.



Figure 7 Example different ages images from FG-NET database

Table 1, Shows the age range distribution of the images that are used in the FG-NET experiment.

Table 1: Age range distribution of the images in the FG-NET Database

Age Range	No of image	FG-NET (%)
0-9	372	37.03
10-19	338	33.83
20-29	144	14.37
30-39	79	7.88
40-49	46	4.59
50-59	15	1.50
60-69	8	0.80

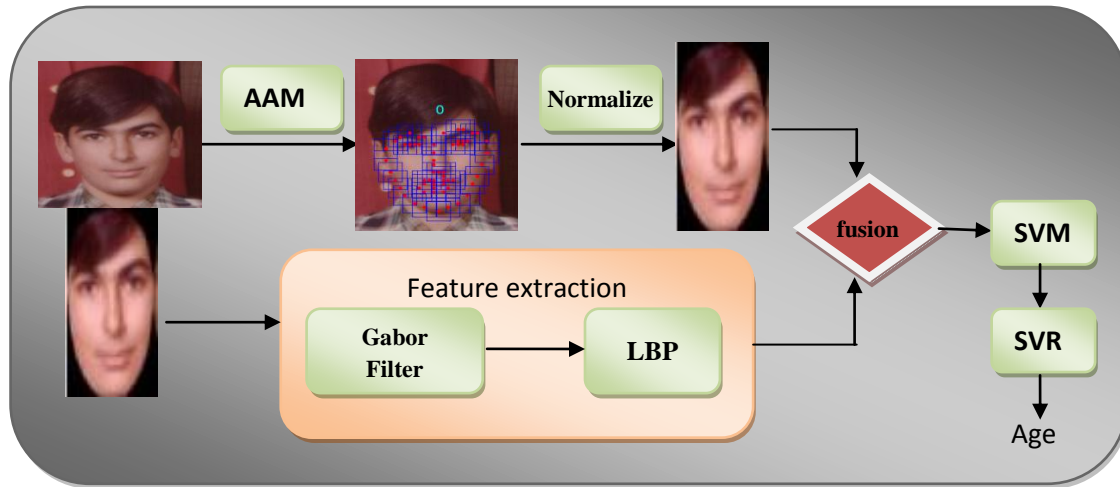


Figure 6 System architecture for proposed age estimation

We evaluate the age estimation performance by Mean Absolute Error (MAE) or Cumulative score (CS)[5]. The MAE is defined as the average of the absolute errors between the estimated ages and the ground truth ages.

$$MAE = \sum_{k=1}^N \frac{|\hat{I}_k - I_k|}{N} \quad (7)$$

Where I_k is the ground truth age for the test image k and \hat{I}_k is the estimated age and N is the total number of test images. The cumulative score $CS(j)$ is defined as $\frac{N_{e \leq j}}{N} \times 100\%$ where $N_{e \leq j}$ is the number of test images on which the age estimation makes an absolute error no higher than j years.

In this experimental work, we evaluate eight approaches for age estimation and compare the MAE of the previously published work with MAE of the proposed approach.

Table 2, Comparisons of the MAE results on the FG-NET Database. First approach that used AAM as geometric extraction method and KNN as classifier. Second use that approach but SVM as classifier. Third approach use SVR as regression method. And the follow approach used AAM to extract geometric feature and LBP for appearance feature and SVM as classifier. Also used the same approach but extract appearance feature by multiple gabor filter with LBP. The last is our approach which uses hybrid AAM and multiple Gabor filter & LBP for extract feature then fusion features for SVM & SVR to estimate age.

Table 2: Comparisons of the MAE results on the FG-NET Database

Algorithm	MAE
AAM +KNN[24]	8.84
AAM+SVM [33]	7.53
AAM+SVR[19,34]	6.02
AAM+LBP+KNN[5,35]	7.29
AAM+LBP+SVM[36]	5.76
AAM+Gabor+LBP+SVM[5]	4.71
AAM+ (Multiple Gabor + LBP) +SVM	3.83
AAM+(Multiple Gabor + LBP) +(SVM +SVR) (Proposed)	3.42

Table 3: Comparisons of MAE at different age ranges on the FG-Net database

Age Group	No. of Images	AAM+ (Multiple Gabor + LBP) +SVM	Proposed
0-9	372	1.74	1.72
10-19	338	3.45	3.31
20-29	144	5.13	4.93
30-39	79	10.54	10.73
40-49	46	10.49	9.89
50-59	15	15.32	14.62
60-69	8	25.63	24.42
Average	1002	3.83	3.42

Table 2, shows that the proposed approach achieves the highest performance in age estimation framework by Mean Absolute Error (MAE) 3.42 because we used the properties of Gabor filter and LBP in the stage of extract appearance feature as well as we used AAM for geometric feature and then using the properties of support vector machine (SVM) & SVR in classification and regression. Compared with the previously reported work [5,19,24,34] in which the experimental settings are similar to ours.

Table 3, Show comparisons of MAE at different age ranges on the FG-Net database for our proposed approach.

7. CONCLUSION

We have presented a hybrid framework for age estimation based on geometric and appearance feature based method. Designing a good filter and classifier is a crucial step for any successful age estimation system. Mean Absolute Error (MAE) 3.42 is achieved under some light intensity and head pose variations. This means that our approach achieves the lowest mean error compared to other approaches in published literature. Using multiple Gabor filters with LBP rendered the method robust to age variations because each filter has specific property to extract. In addition using generalization property of SVM and SVR classifier And regression increased the recognition rate in presence of age class variations.

We believe that age estimation system under varying conditions is still an interesting area of research, and we anticipate that there will be many further advances in this area.

REFERENCES

- [1] Y. Fu, G. Guo, and T. S. Huang, "Age synthesis and estimation via faces: A survey," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 32, no. 11, pp. 1955–1976, 2010.
- [2] A. Lanitis, C. Draganova, and C. Christodoulou, "Comparing different classifiers for automatic age estimation," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 34, no. 1, pp. 621–628, 2004.
- [3] Liu K-hsien, Yan S, Member S, Kuo CJ." Age Estimation via Grouping and Decision Fusion". *IEEE Transactions on Information Forensics and Security*. 2015.
- [4] Guo G, Member S, Fu Y, et al. Image-Based Human Age Estimation by Manifold Learning and Locally Adjusted Robust Regression. *Image (Rochester, N.Y.)*. 2008;17(7):1178-1188.
- [5] Eun S, Joo Y, Joo S, Ryoung K, Kim J. Age estimation using a hierarchical classifier based on global and local facial features. *Pattern Recognition*. 2011;44(6):1262-1281. Available at: <http://dx.doi.org/10.1016/j.patcog.2010.12.005>.
- [6] Y. Fu, Y. Xu, and T. S. Huang, "Estimating human ages by manifold analysis of face pictures and regression on aging features," in *Proc. IEEE Conf. Multimedia Expo.*, 2007, pp. 1383–1386.
- [7] Rania S. El-sayed, M. Y. El-Nahas, A. El Kholy "Robust Facial Expression Recognition via Sparse Representation and Multiple Gabor filters". *IJACSA*. 2013;4(3):82-87.
- [8] Y. Kwon and N. Lobo, "Age classification from facial images," *Comput. Vis. Image Understand.*, vol. 74, no. 1, pp. 1–21, 1999.
- [9] Guo G, Dyer C. "A Study on Automatic Age Estimation using a Large Database". *Young. (C)*.
- [10] N. Ramanathan and R. Chellappa, "Modeling age progression in young faces," in *Proc. IEEE Conf. CVPR*, 2006, pp. 387–394.
- [11] X. Geng, Z.-H. Zhou, Y. Zhang, G. Li, and H. Dai, "Learning from facial aging patterns for automatic age estimation," in *Proc. ACMConf. Multimedia*, 2006, pp. 307–316.
- [12] Y. Fu and T. S. Huang, "Human age estimation with regression on discriminative aging manifold," *IEEE Trans. Multimedia*, to be published.
- [13] K. A. Deffenbacher, T. Vetter, J. Johanson, and A. J. O'Toole, "Facial aging, attractiveness, and aistinctiveness," *Perception*, vol. 27, pp. 1233–1243, 1998.
- [14] T.F. Cootes, G.J. Edwards, C.J. Taylor, Active appearance models, *IEEE Transactions on Pattern Analysis and Machine Intelligence* 23 (6) (2001) 681–685.
- [15] A. Gunay, V.V. Nabyeyev, Automatic age classification with LBP, in: 23rd International Symposium on Computer and Information Sciences, ISCIS 008 (2008) 1–4.

- [16] S. Yan, H. Wang, T. S. Huang, and X. Tang, "Ranking with uncertain labels," in Proc. IEEE Conf. Multimedia and Expo, 2007, pp. 96–99.
- [17] S. Yan, H. Wang, X. Tang, and T. S. Huang, "Learning auto-structured regressor from uncertain nonnegative labels," presented at the IEEE Conf. ICCV, 2007.
- [18] Lanitis A. An Overview of Research on Facial Aging using the FG-NET Aging Database. 2015;(MAY).
- [19] Liu J, Ma Y, Duan L, Wang F, Liu Y. Hybrid constraint SVR for facial age estimation. Signal Processing. 2013;1-7. Available at: <http://dx.doi.org/10.1016/j.sigpro.2013.07.025>.
- [20] Günay A, Nabiye VV. Age Estimation Based on AAM and 2D-DCT Features of Facial Images. International Journal. 2015;6(2):113-119.
- [21] Jun-Da Xia, Chung-Lin Huang, Age estimation using AAM and local facial features, in: International conference on Intelligent Information Hiding and Multimedia Signal Processing (2009) 885–888
- [22] Laskar BZ, Majumder S. Artificial Neural Networks and Gene Expression Programming based age estimation using facial features. Journal of King Saud University - Computer and Information Sciences. 2015. available at: <http://dx.doi.org/10.1016/j.jksuci.2014.06.017>.
- [23] Hironori Takimoto, Yasue Mitsukura, Minoru Fukumi, Norio Akamatsu, Robust gender and age estimation under varying facial pose, Electronics and Communications in Japan 91 (7) (2008) 32–40
- [24] Chao W-lun, Liu J-zuo, Ding J-jiun. Facial age estimation based on label-sensitive learning and age-oriented regression. Pattern Recognition. 2013;46(3):628-641. Available at: <http://dx.doi.org/10.1016/j.patcog.2012.09.011>.
- [25] M.A. Turk, A.P. Pentland, Eigenfaces for recognition, Journal of Cognitive Neuroscience 3 (1) (1991) 71–86.
- [26] Jana R, Datta D, Saha R. Age Estimation from Face Image using Wrinkle Features. Procedia - Procedia Computer Science. 2015;46(Icict 2014):1754-1761. Available at: <http://dx.doi.org/10.1016/j.procs.2015.02.126>.
- [27] X. Geng, K. Smith-Miles, Z.H. Zhou, Facial age estimation by learning from labeled distributions, in: Proceedings of the AAAI Conference on Artificial Intelligence, 2010, pp. 451–456.
- [28] A. R. Webb. Statistical Pattern Recognition, 2nd Edition. John Wiley, 2002.
- [29] R. O. Duda, E. H. Peter, and G. S. David, Pattern Classification, 2nd ed. New York: Wiley Interscience, 2000.
- [30] Timo Ahonen, Abdenour Hadid, Matti Pietikainen, Face recognition with local binary pattern, Lecture Notes in Computer Science 3021 (2004) 469–481.
- [31] Timo Ojala, Matti Pietikainen, M. Pietikainen, "Multiresolution Gray-scale and rotation invariant texture classification with local binary patterns, IEEE Transactions on Pattern Analysis and Machine Intelligence 24 (7) (2002) 971–987.
- [32] X. Geng, Z.-H. Zhou, and K. Smith-Miles. "Automatic age estimation based on facial aging patterns". IEEE Trans. on PAMI, 29(12):2234–2240, 2007.
- [33] G. SK, N. SH. Human Age Estimation Framework using Bio-Inspired Features for Facial Image. International Journal of Engineering. 2015;4(7):85-88.
- [34] Luu, K., Ricanek, K., Bui, T. D., Suen, C. Y.: 'Age estimation using active appearance models and support vector machine regression'. Proceedings IEEE third International Conference on Biometrics: Theory, Applications, and Systems, 2009, pp. 1-5.
- [35] Street A. HUMAN AGE ESTIMATION VIA GEOMETRIC AND TEXTURAL. Computer. 2008.
- [36] Han H, Otto C, Jain AK, Lansing E. Age Estimation from Face Images : Human vs . Machine Performance. Aging. 2013.

A Joint Port and Statistical Analysis Based Technique to Detect Encrypted VoIP Traffic

Suneel Munir^{1*}, Nadeem Majeed², Salaser Babu³, Irfan Bari⁴, Jackson Harry⁵, Zahid Ali Masood^{6#}

^{1,2,3,4,5} University of Engineering & Technology, Taxila

⁶COMSATS Institute of Information Technology, Islamabad

Abstract

VoIP is rapidly growing technology due to its cost effectiveness, dramatic functionality over the traditional telephone networks and its compatibility with public switched telephone network (PSTN). Detection of VoIP is important for telecommunication authorities, internet service providers, and governmental law enforcement agencies for blocking, prioritizing, monitoring and electronic surveillance. Modern VoIP applications use dynamic ports, proprietary protocols, encryption, obfuscation and anti reverse-engineering procedures leaving port-based techniques, signature-based techniques and pattern-based detection ineffective. For generic purpose, only statistical techniques can be used for better results but existing statistical analysis-based detection techniques have some limitations and cannot provide more efficient and accurate solutions. In this paper, we proposed a hybrid solution based on port number and statistical analysis using threshold values of flow statistical parameters to detect the VoIP media (voice) flows. The solution is generic, efficient, accurate, real time (to some extent) and can detect encrypted, plain and tunneled VoIP traffic. The proposed system is evaluated for accuracy, efficiency, and scalability. It has 97.165% detection rate (DR) and 2.68% false positive rate (FPR). It can detect VoIP calls from any VoIP application or protocol within 6 seconds. The proposed system shows better results and hence can fulfill the need of telecom operators and ISPs for detecting VoIP.

Keywords: VoIP, Encryption, Statistical analysis, Flow, Detection Rate (DR), False Positive Rate (FPR)

1. Introduction

Voice over Internet Protocol (VoIP) usage is increasing day by day due to its low cost and dramatic functionalities. The adoption of VoIP is not without its complications. The commercial usage of VoIP is prohibited in many countries, as it incurs loss in profit to their telecommunication industries. Internet service providers also desire to prioritize VoIP for their paid customers. Government and law enforcement agencies are also concerned in tracking down VoIP traffic in real time to counter any vicious activity. Not only this, many VoIP applications are prone to number of P2P vulnerabilities such as buffer overflow and denial of service attacks. VoIP applications also make direct connections with unknown clients so they can be exploited by viruses, worms and Trojan. All these problems affect the productivity and efficiency of large organizations. So detection of VoIP has become a hot area of research. Use of complex encryption and tunneling mechanisms for VoIP makes detection very difficult. VoIP signaling and media transmission both may be encrypted or any one may only be encrypted. Different techniques exist to detect VoIP traffic. These techniques are divided into 6 basic classes i.e. port-based, signature-based, pattern-based, statistical analysis-based, machine learning based, and hybrid detection techniques. Each type of technique has some limitations. Some of these techniques are rarely used nowadays, due to complex, confidential and secure privacy protocols. Also with the development of new VoIP applications and technologies, the detection of VoIP is becoming

more and more difficult. So it is very hard to come up with a solution that can detect VoIP with 100% of accuracy and efficiency.

In this paper we proposed a hybrid solution based on port number and statistical analysis using threshold values of flow statistical parameters to detect the VoIP media (voice) flows. The solution is generic, efficient, accurate, real time (to some extent) and can detect encrypted, plain and tunneled VoIP traffic. The remainder of this paper is organized as follows. In Section 2 we briefly describe related work. In Section 3 we introduce our classification methodology, showing how we carried out statistical analysis and what observations we took to build our own proposed system. Section 4 is about proposed system, which describes threshold rules and algorithms to detect VoIP and non-VoIP traffic. In Section 5 we evaluated our system for accuracy, efficiency and scalability. Finally Section 6 concludes the paper.

2. Related work

The main steps that are involved in VoIP call setup are signaling and media channel setup (voice transmission). The detection techniques can be applied on any of these two steps. Some techniques detect VoIP traffic by examining signaling traffic and others detect VoIP by examining media traffic. Some techniques exist that examine both signaling and media traffic. In this section we provide basics of VoIP and moreover we review existing VoIP detection techniques and approaches and the recent work that has been done using these techniques. There are basically 6 types of techniques that are used to detect VoIP traffic flows.

2.1 Port based detection techniques

The simplest, robust and fastest of the detection technique is port based detection. This approach allows fast flow classification because port number can be easily accessed and are generally not affected by encryption. Table 1 shows some of standard ports for specific VoIP applications by IANA.

Sr. No.	VoIP Protocol	Port Number	Default Transport Layer Protocol
1	SIP	5060-5070	TCP/UDP
2	H.323	1718-1720	TCP/UDP
3	MGCP/Megaco /H.248	2427,2944	TCP/UDP
4	Skype(client login)	80,443	TCP
5	Skype (authentication)	33033	TCP

Table 1: VoIP protocol and standard ports specified by IANA

By port-based analysis if these ports are used at transport layer, the flow is detected as VoIP. Leung et al, in [1] used port numbers as helping information to detect VoIP. Renal et al, in [2], detected Skype VoIP traffic by matching distinct Skype keywords, ports, and content. Port based detection techniques are easy to implement and fast but less accurate as non standard ports are used by modern VoIP applications. Moreover the ports are dynamically allocated and in case of IP layer tunnels, the transport layer information is hidden. So in these cases this technique is useless and produces incorrect results

2.2 Signature based detection techniques

Signature-based techniques are also called as protocol decoding techniques. A signature-based detection method classifies the internet traffic by matching specific strings within packet payload for that protocol [3]. It detects VoIP using deep packet inspection. Each VoIP protocol has distinct signatures that can be used for detecting VoIP traffic. Signature-based detection techniques in [2, 4-6] detect VoIP flows by VoIP application signatures. Renal et al, in [2] proposed a signature based approach to block Skype traffic. They discovered that the Skype packets contain the keyword `"/getlatestversion?ver="` or `"/getnewestversion"` combined with a `"/ui/"` string. Table 2 shows some distinct signatures of various VoIP protocol and applications. The signature-based detection techniques are easy to implement, fast and efficient for un-encrypted data but these are ineffective for encrypted and tunneled data as it modifies the signatures.

Sr. No.	VoIP Protocol	Signature	Place to Find
1	SIP	“sip”	Application data
2	RTP/SRTP	0x80,0x81	RTP header, after transport layer Header
3	ZRTP	“1000xxxx5a525450	header, Payload
4	Skype login	“16 03 01 00 ** 42 cd ef e7 40 d7”	Payload, within transport layer Packet
5	Skype (contents)	“/getlatestversion?ver=”	Payload, within transport layer packet

Table 2: VoIP protocols and applications signatures

2.3 Pattern based detection techniques

Pattern based detection techniques are proposed to handle the shortcomings of port and signature based detection techniques. In Pattern-based detection techniques the particular pattern of signals between communication parties is identified. These techniques are powerful for the detecting those VoIP applications that use proprietary protocols for signaling i.e. Skype. Pattern based detection techniques are proposed in [1, 4, 6, 7]. In [1] pattern based detection along with port based detection is proposed to detect Skype Traffic. The researcher used forensic approach to investigate the Skype by deeply investigating the Skype communication. They also discussed 15 basic stages of Skype communication from start to end. Feng et al, in [4] used a joint port-based and pattern-based techniques to detect VoIP traffic. They analyze the Skype protocol with respect to its general and behavioral characteristics and used them to identify the Skype traffic to block it. Uzma et al. [7] in 2014 proposed a pattern based approach to detect illegal VoIP traffic using Call Detail Records. They used sip signature “sip” in the Skype signaling traffic to identify VoIP traffic. Pattern based detection techniques works well in some cases to detect encrypted VoIP but they are dependent on specific VoIP application. The signaling mechanism may vary from application to application, making it less accurate and inefficient.

2.4 Statistical analysis based detection techniques

Traffic classification techniques which need to access the payload of the packets do not work always for the identification of all protocols. Indeed, in order to protect the user's privacy, some legal restrictions are imposed to prevent the access to the payload of the packets. Not only this, if the payload of the packet is encrypted, the access to the payload is also prevented. To overcome all these limitations, the statistical analysis based detection approaches came into research [3, 8-17]. By statistical techniques, some statistical measures are taken on flow features such as mean, standard deviation (S.D) of packet sizes and the packet arrival time measures are used for VoIP detection. Statistical analysis is mostly performed on voice data but it can also be performed on signaling data. Yildirim et al.[10] in 2010 proposed a simple VoIP traffic classification method. The authors used the packet length as the statistical measure to mark a packet. They proposed that the packet will be a VoIP packet if its size is between 60 and 150 bytes. Piskac et al. in [16] proposed a statistical method to classify traffic using the time characteristics of the data flow. Statistical measures like number of packets and their size in bytes, S.D, Mean, minimum difference, maximum difference of the inter-arrival time of packets in a flow are used to classify VoIP traffic. On bases of these values the vector for each packet and each flow is formed. The authors also used Euclidean distance, Root-Mean-Square distance and the angles between the vectors to calculate the associations between the different vectors. The proposed approach has TPR of about 90% and FPR of 7% respectively. Fauzia et al, in [11] proposed a generic technique to detect the VoIP traffic generated by different VoIP protocols. They perform some statistical analysis on the traffic and separate out the VoIP media traffic by using traffic features that are difficult to alter such as packet interval time, packet sizes, rate of exchange. Freire et al, in [12] proposed a solution that detects the VoIP calls hidden in web traffic such as Gtalk and Skype traffic. The authors analyzed the media traffic by taking parameters such as web request size, web response size, inter arrival time between requests, no. of requests per page, page retrieval time. They use goodness of fitness test, the Kolmogorov-Smirnov (KS) distance and chi-square values and obtain metrics to identify the VoIP in web traffic. The scheme considers the key

characteristics of normal behavior of web traffic (HTTP, HTTPS) and matched it to the actual traffic to identify VoIP. Yildirim et al. proposed statistical technique [10] to identify VoIP protocol within encrypted tunnel. They use probabilistic information of traffic to identify application protocols in tunnels. Their decision algorithm does Packet size distribution on packets that lies with a specified size range. Ying-Dar et al. [8] also proposed a generic technique to classify the network traffic into different application types. They use packet size distribution (PSD) and assume that each application has a distinct PSD. They also use the port association techniques while classifying traffic by which if a port is consecutive to the previously identified flow port then it is detected as the part of the previous flow. Toshiya et al, [15] in 2006 proposed Flow level behavior (FLB) VoIP detection technique. They also used packet size and inter-arrival time to classify VoIP traffic.

2.5 Machine learning based detection techniques

In addition to normal statistical analysis for data classification, many researchers are now interested in heuristics and statistical-based traffic classification using machine learning algorithms. Machine learning algorithms can create a data model from a given dataset automatically. The created data model comprises of a decision tree or a decision table which selects the best suitable attributes and threshold values for data classification. Machine learning based detection techniques are discussed in [18-26]. Riyad et al. [26] used ML to detects the VoIP traffic by using flow features, such as size and time. They evaluated the three different machine learning (ML) algorithms C4.5, AdaBoost and Genetic Programming (GP) under data sets common and independent from the training condition. Two VoIP applications Skype and Gtalk are tested. Their result shows that C4.5 has the best performance with DR 99% and FPR less than 1%. Riyad et al. [21, 25] extended their previous research work to detect encrypted VoIP traffic by using machine learning techniques. They applied three ML algorithms to test more data traces produced by different application. They deployed three supervised learning algorithms, namely C5.0, AdaBoost and Genetic Programming (GP), to generate signatures automatically to robustly classify VoIP encrypted traffic. Their results show that C5.0

performs much better than GP and AdaBoost algorithms in detecting encrypted VoIP traffic. They demonstrate that C5.0 algorithm can also accurately differentiation between multiple VoIP applications without employing port numbers, IP addresses and payload information. Lam H et al, [27] in 2009 proposed a machine learning based traffic detection system to classify Skype, VoIP and other traffic. They used packet length and inter-arrival time between packets as statistical features to identify VoIP flows. Despite calculating statistical parameters on complete flow they used short sliding window of 10 seconds. The proposed solution is almost real time, producing accuracy of 99%. Zander et al, [18] in 2005 proposed ML based traffic classification and application identification technique by using an unsupervised machine learning. The researcher used (SFS) Sequential Forwarding Selection to find the best attributes from the dataset. The statistical attributes considered were packet inter-arrival time, packet length mean, packet length variance and flow size in bytes. To evaluate the quality of results a metric called as intra-class homogeneity H. Higher homogeneity H was required for better traffic classification. The average accuracy of their proposed technique was 86.7%. Support Vector Machine (SVM) is considered as one of the best machine learning algorithm for classification purpose. SVM has some distinctive features, such as small sample sets, high accuracy, ability for simultaneously minimizing the empirical classification error and maximizing the geometric margin classification space and strong generalization performance. Beside network traffic classification it can be applied to text categorization, image recognition and motion classification. SVM based ML techniques in [23, 24] are used for traffic classification. S. Anu et al. [24] in 2014 proposed Support Vector Machine (SVM) based network traffic classification technique. The researchers compared the classification performance of SVM with Naive Bayes, C4.5 and K-NN method. Their result shows that SVM has better classification accuracy than other three models. Statistical approaches are good and produce better results in case of encrypted VoIP. The results of statistical approaches are better than other approaches on latest VoIP applications but still the existing statistical techniques are not so efficient for IP layer tunneled VoIP detection. Moreover most of the statistical approaches are not

real time and need prior captured traffic to analyze. So these systems could not be practically implemented to block or prioritize VoIP efficiently and accurately with best results.

2.6 Hybrid detection techniques

To gain the advantages of multiple approaches and overcoming the limitations of above mentioned techniques, the hybrid VoIP detection techniques are proposed. The hybrid techniques produce better results than individual technique. Hybrid detection techniques are discussed in [1, 6, 28] [18, 19, 24, 25]. Pattern-based analysis with port-based analysis are used in [18, 19] for Skype traffic detection. D. Adami et al, in [29] proposed a pattern and a port-analysis based hybrid technique to detect Skype traffic. The author analyzed Skype for Skype UDP

ping, Skype UDP probe, Skype TCP handshake, and Skype authentication both statistically and behaviorally.

D. Adami et al, in [28] proposed a hybrid technique for detecting Skype traffic. Both signature-based and statistical approaches are used in parallel producing best results. The proposed system outperforms the classical statistical analysis based detection classifiers as well as the state-of-the-art ad hoc Skype classifier. Robert B. et al, in [30, 31] presented an extensive measurement campaign focusing on VoIP traffic characterization. The researcher proposed a heuristic algorithm based on joint signature, port and statistical analysis based hybrid techniques to identify RTP/RTCP traffic.

The comparison of discussed techniques is shown in Table 3

Detection Technique	Applied on	Scalability	Performance Speed	Encryption support
Port based	Signaling, voice	Application and Protocol Specific	Good	Yes, other than IP tunneling
Signature based	Signaling, voice	Application and Protocol Specific	Better	No
Pattern based	Signaling	Application and Protocol Specific	Better	Limited
Statistical analysis based	Mostly on voice	Generic	Bad	Yes
Machine Learning	Mostly on Voice	Generic	Bad	Yes
Hybrid	Signaling, Voice	Generic	Bad	Yes

Table 3: Comparison of VoIP Detection Techniques

Each of the discussed technique has some limitations. Statistical, machine learning and hybrid detection techniques normally works well in generic. So there is a need of an accurate, generic, efficient, real time and practically implementable statistical analysis-based or hybrid solution that can detect encrypted, non-encrypted and tunneled VoIP. The detection algorithm should not be dependent on any VoIP application, protocol, security mechanism, or any tunneling mechanism.

3. Methodology

We considered the most famous VoIP applications of modern days, and analyzed the traffic traces produces by them. The data for traffic analysis is obtained from NARC of University of engineering and technology Taxila, home users, sample traces from Wireshark and tstat sites.

For experimental analysis we considered the traffic traces of common VoIP applications like facebook messenger, viber, skype, google hangouts and

yahoo messenger as testing applications. In addition to these applications, traffic traces of various non-VoIP applications and services are also analyzed such as online gaming, torrents (bittorrent, utorrent), antivirus updates (MS Security Essentials, Kaspersky), online streaming/online tv, audio video streaming, download Manager, FTP, chat applications (Yahoo, Gmail, MSN), web browsing and Emailing. We used wireshark and weka as analysis tool.

3.1 Statistical analysis

The main statistical parameters we are used to analyze each flow are, packet-rate, mean and standard deviation of packet sizes, maximum difference time, mean and standard deviation of maximum difference time, entropy and data rate. : No. of packets in seconds. Packet rate of the flow in packets/sec

- Mean(Avg. size) : Mean (average) of IP layer (layer 3) packets sizes of the flow in bytes
- S.D (size): Standard deviation of IP layer (layer 3) packets sizes of the flow in bytes
- Max-diff-time: Maximum difference between the current and previous packets' time for all packets of the flow in seconds

- Mean(diff-time): Mean (average) of the difference between the current and previous packets times in seconds
- S.D (diff-time): Standard deviation of the difference between the current and previous packets times of the flow in seconds
- Data rate: No. of Mbs in seconds.
- Entropy (H): Measure of the degree of uncertainty of a given random variable

The statistical analysis is performed on traces by two ways; firstly, the statistical parameters are calculated and analyzed for each flow of complete session without considering time limit. In real circumstances, it makes no sense to identify Internet flows when they have ended. The early identification of the flow is very essential to apply the subsequent management and security policies. In the second phase we analyzed statistical parameters of each flow by adopted sliding window of 5 seconds, means data for first 5 seconds of the each flow is captured and analyzed. Table 4 and 5 shows statistics of VoIP and non-VoIP traffic traces.

Statistical Parameters	Google + hangouts	Facebook VoIP	Yahoo messenger	Skype 7.2.2	Viber
Time	3m21s	2m46s	2m6s	5min	1m42s
Packets	15200	4101	5200	30367	7322
Packet rate(p/sec)	68	24.7	41.27	101	71
Mean (P_Size)	73.5	107	92	135	130
S.D (P_Size)	38.88	41.115	18	28	41.26
Max_diff_time	0.19	0.232	0.099	0.138	0.39
Mean(diff_time)	0.055	0.069	0.0299	0.028	0.0477
S.D(diff_time)	0.041	0.045	0.022	0.026	0.048
Data Rate (Mb/sec)	0.481	0.028	0.031	0.119	0.074
Entropy (H)	3.29	2.78	3.17	3.77	8.24

Table 4: Statistical results of VoIP traffic traces

Statistical Parameters	Online TV	torrent	Yahoo text chat	Game play	Youtube	Antivirus update	Download Manager/FTP	Web Browsing
Time	3m2s	3m40s	3m52s	9m5s	1m39	1m20s	5mins	2m52s
Packets	39476	145984	208	1145	8671	529	148434	4646
Packet rate (p/sec)	78	663	0.89	31	87	6.612	495	27
Mean(P_size)	746	845	168	581	876	386	1034	506
S.D(P_size)	106	117	40	653	683	593.18	663.5	598
Max_diff_time	0.331	0.475	0	0.341	0.177	0.254	0.426	0.343
Mean(diff_time)	0.023	0.047	0	0.024	0.009	0.023	0.047	0.0295
S.D(diff_time)	0.0588	0.097	0	0.061	0.232	0.058	0.094	0.0738
Date Rate (Mb/s)	0.331	3.978	0.001	0.0031	0.616	0.051	4.088	0.109
Entropy (H)	0.882	1.866	2.01	1.287	0.773	0.014	1.445	1.357

Table 5: Statistical results of non-VoIP traffic traces

3.2 Key observations from statistical analysis

From the statistical analysis we noticed following findings

a. The average packet size and standard deviation of VoIP data is much smaller than non-VoIP.

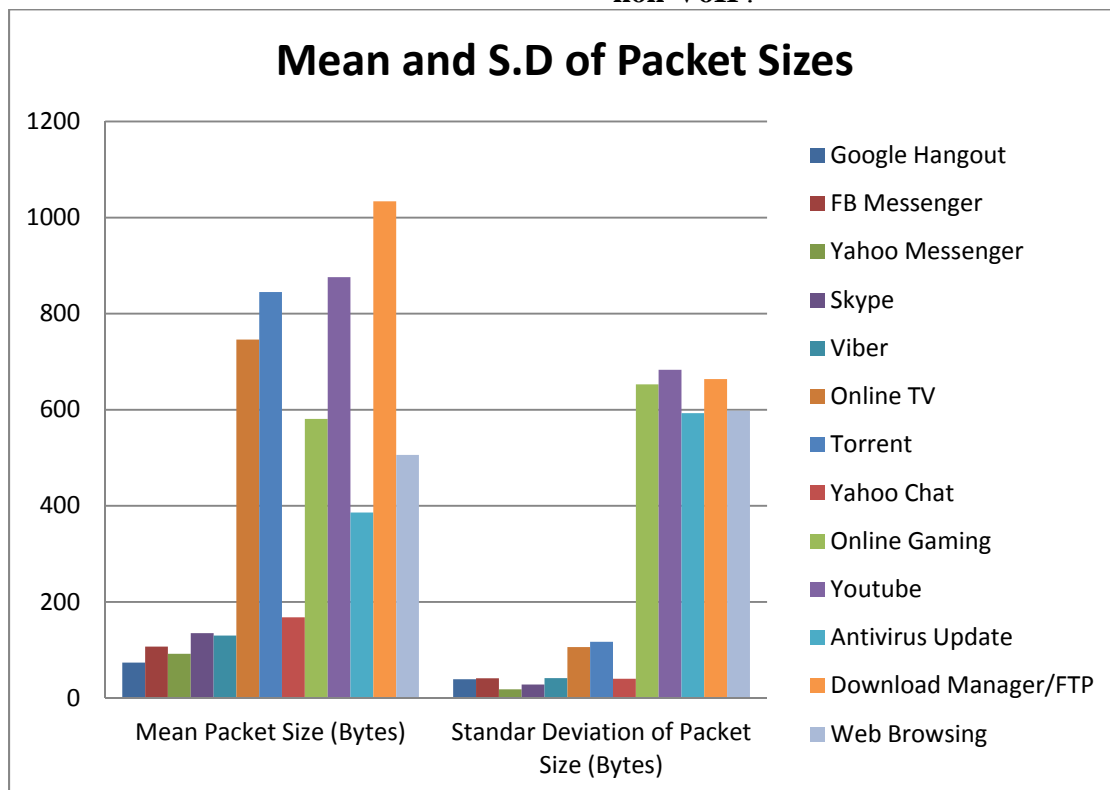


Figure 1: Mean and S.D of VoIP and non-VoIP traffic traces

b. The packet rate of VoIP is greater than some non-VoIP applications

The packet rate of non-VoIP chat applications, web browsing and antivirus update is lower than VoIP.

On the other hand torrent and download managers have higher packet rates.

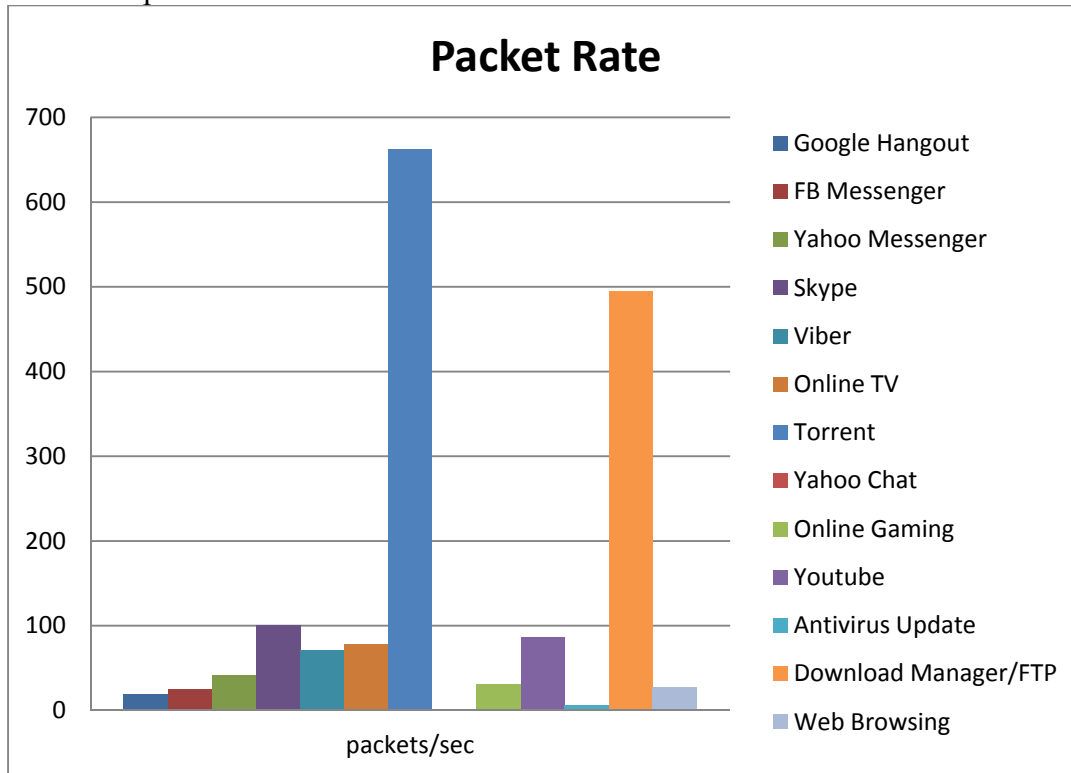


Figure 2: Packet rate of VoIP and non-VoIP traffic traces

c. The entropy (H) of VoIP is greater than non-VoIP traffic traces

Entropy has been used in different fields of study and therefore has several interpretations. It is defined as measure of the degree of uncertainty of a given random variable. Entropy is denoted by $H(n)$

where n represents number of values in the observation pool, and $p(x_i)$ denotes the probability of occurrence of a given value x_i . Entropy is represented by the expression (1).

$$H(X) = -\sum_{i=0}^n p(x_i) \ln(p(x_i)) \quad (1)$$

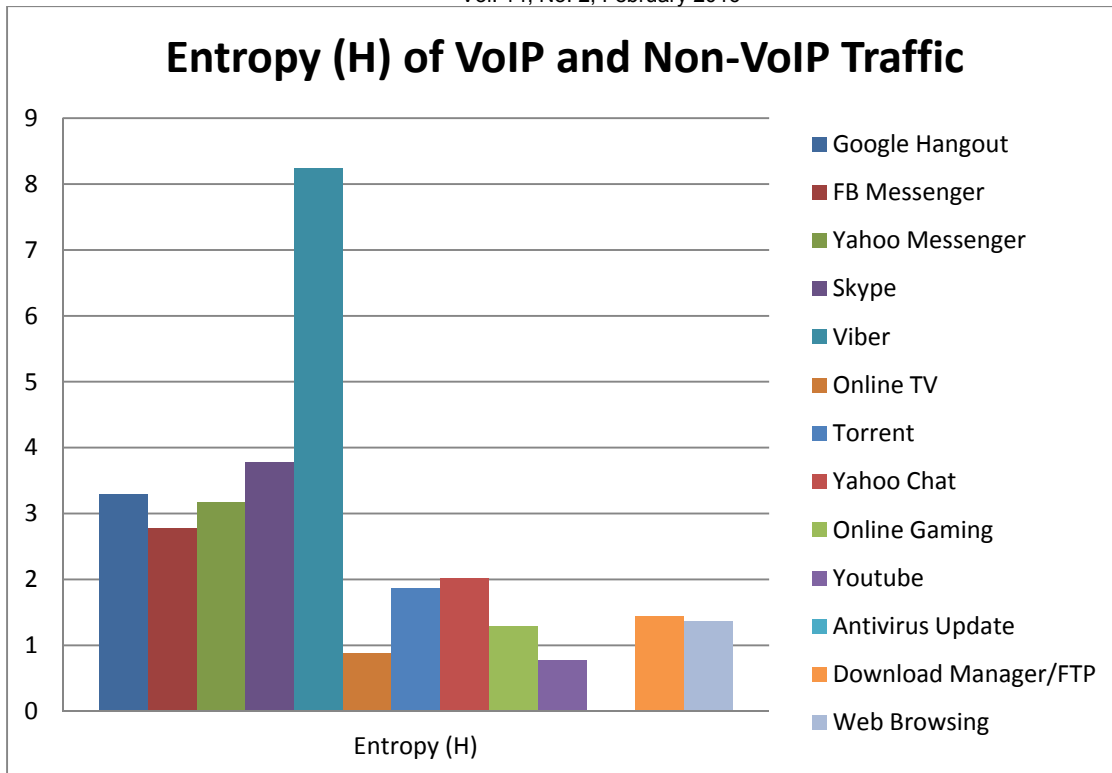


Figure 3: Entropy of VoIP and non-VoIP traffic traces

d. The data rate of VoIP is smaller than some of non-VoIP data.

Torrents and download managers have higher data rate than VoIP.

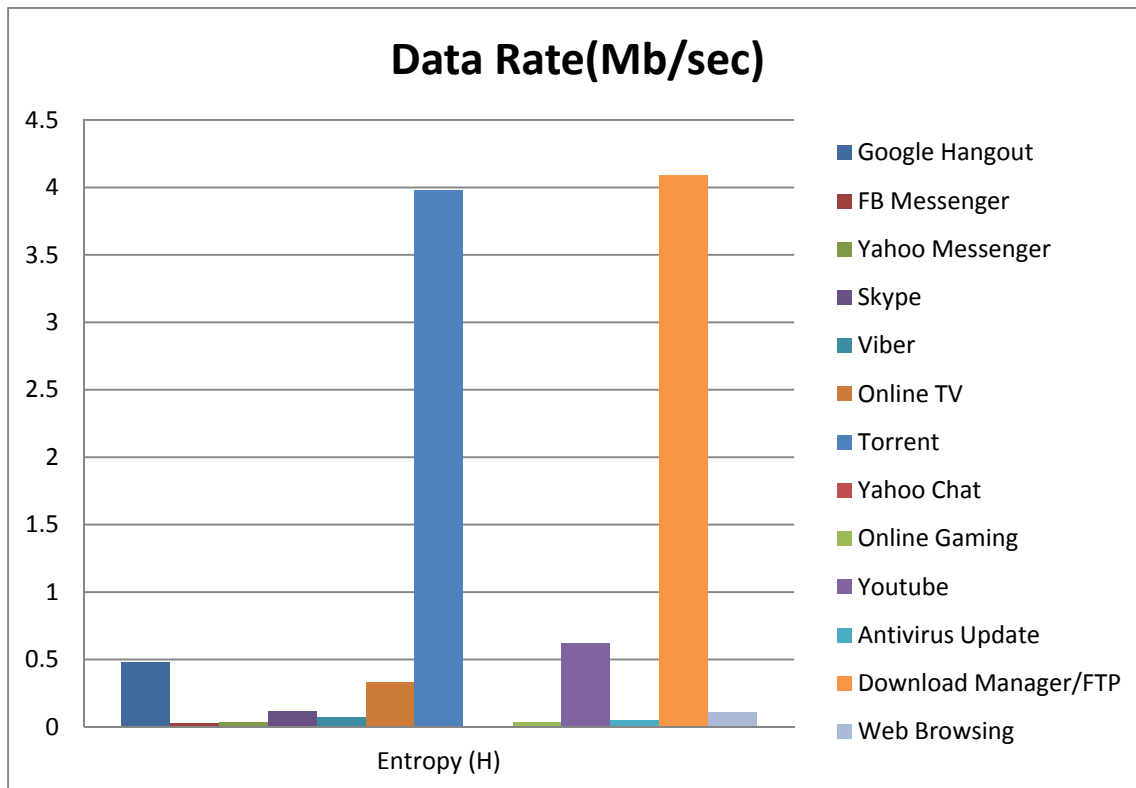


Figure 4: Data rate of VoIP and non-VoIP

4. Proposed System

On the bases of experimental analysis we proposed a system which can identify VoIP efficiently and accurately.

4.1 Flow registration process

Firstly each flow is registered. The proposed system distinguishes each flow by 4 tuples (Source-IP, Destination-IP, Source Port, and Destination Port). It is useless to identify the flow after it has been

1. Packet Rate > 15 packets/sec
 2. Data Rate < 0.5 Mb/s
 3. $50 \leq \text{Mean}(\text{packet size}) \leq 210$ bytes
 4. $0 \leq \text{S.D}(\text{packet size}) \leq 75$ bytes
 5. $\text{Mean}(\text{packet size}) \geq \text{S.D}(\text{packet size})$
 6. $\text{Mean H}(\text{Packet Size}) \geq 3.0$
-
7. $0 < \text{max-diff-time} \leq 0.8$ seconds
 8. $0 < \text{Mean}(\text{diff-time}) \leq .09$ seconds
 9. $0 < \text{S.D}(\text{diff-time}) \leq 0.25$ seconds

All 6 rules must be true

At least 2 rules from 3 must be satisfied

Figure 5 shows the flow diagram of VoIP detection process. If first 6 rules are true and none of the last three rules are satisfied then the flow is re-registered again. The traffic of next five seconds of the particular flow is captured again and statistics are calculated. If none of the last three rules are satisfied for three times, then the flow is marked as non-VoIP.

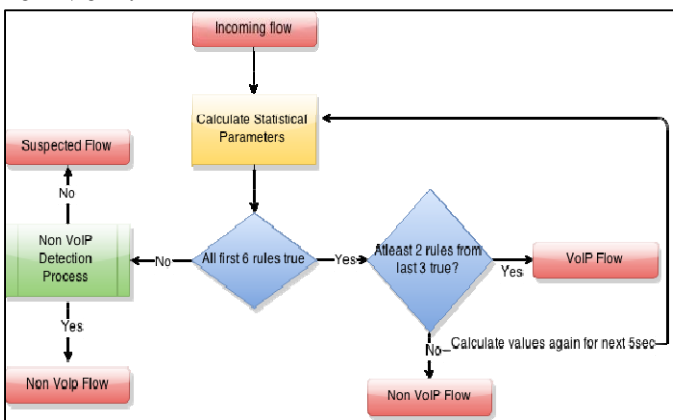


Figure 5: VoIP detection Process

4.3 Non-VoIP detection process

If any of first 6 rules is false then non-VoIP process is called to verify it as non-VoIP or suspected flow. From statistical analyses we have noticed that some of non-VoIP applications do satisfies rule 1 and 2. If first two rules are true and none of the rules from 3, 4, 5, and 6 are satisfied then the flow is termed as

ended. Therefore we focus our research on early identification. For this purposes the traffic of first 5 seconds for each flow is captured to calculate the statistics. After flow is registered, set of rules are applied to it to identify the flow as VoIP or non-VoIP. We set these nine rules for VoIP traffic detection.

4.2 VoIP detection process

A flow will be VoIP if all first 6 rules are true and if it satisfies 2 from last 3 rules.

non-VoIP flow otherwise it is termed as suspected flow. A suspected flow is one that cannot be identified as VoIP or non-VoIP. It means that the system is unable to decide and evaluate the flow. Figure 6 show the flow diagram of non-VoIP detection process.

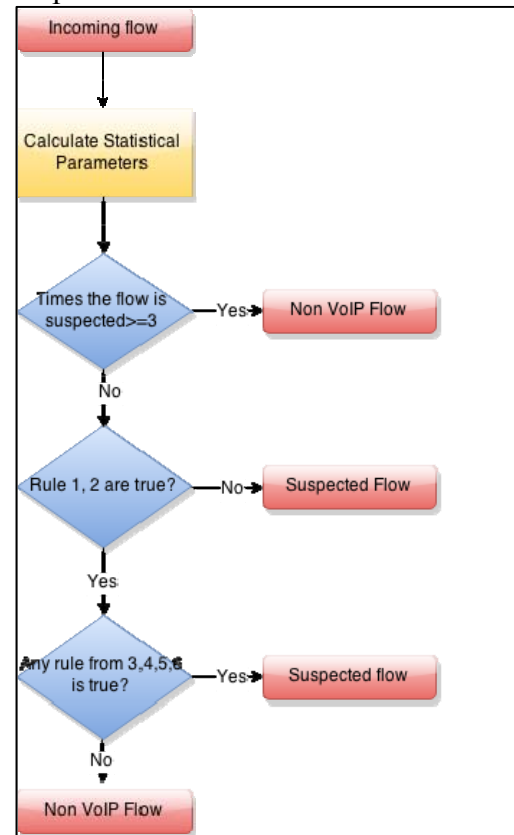


Figure 6: Non-VoIP detection process

4.4 Proposed system for detecting VoIP in IPSec tunnels

Internet Protocol Security (IPsec) is a protocol suite that secure the Internet Protocol (IP) communication by encrypting and authenticating each IP packet of a communication session [32]. IPsec operates in two modes, transport mode and tunnel mode. Payload data is encrypted in transport. When IPsec operates in tunnel mode, the whole IP packet is encrypted, authenticated or both, which means that IP packet is encapsulated into a new IP packet with a new IP header. The new IP header hides the transport layer information and hence we will have no knowledge of transport layer ports. The only available information is IP layer information so to detect VoIP in IPsec tunnel the proposed system needs little variation. Instead of distinguishing flows by 4 tuples (S-IP, SP, D-IP, DP) we will distinguish flows by 3 tuples (S-IP, D-IP, SPI). Security Parameter Index (SPI) is an essential part of IPsec which serves as an identification tag added to the header. SPI works like works like port numbers in TCP and UDP connections. For each flow we calculate statistical parameters and implement all nine rule mentioned

in section 4.1. The same detection algorithm is used for detection of VoIP flows hidden in IP Layer tunnels with slight variations. The main points that are different from previous algorithm are as follows:

- i. Each flow will be distinguished by 3 tuple (S-IP, D-IP, SPI)
- ii. Remove the size of IPsec headers from overall IP Layer packet size while calculating statistical parameters related to size.
- iii. Rest of algorithm will be same.

5 Performance evaluation of proposed system

To evaluate our proposed system w.r.t accuracy, efficiency and scalability, we implemented it in C++ using winpcap library. We collected different datasets and captured network traces from different locations such as tstat[33] and wireshark[34] sites. We also captured our own VoIP and non-VoIP traffic traces for evaluation. Table 6 and 7 shows the traffic traces for evaluating performance of the proposed system.

Trace	Codec	Transport Layer protocol	Size (MB)	Duration (Sec)
E2E-140606-1	G729	UDP	8	905
E2E-140606-1	iLBC	UDP	11	1003
E2E-140606-3	iSAC	UDP	12	1116
SkypeOut-260906-1	G729	TCP	9	919
SkypeOut-260906-1	G729	UDP	8	910
Internet-E2X-29		TCP	207	343546
Internet-E2E		UDP	4GB	344700
Internet-E2O		UDP	264	343562

Table 6: Downloaded traffic traces from tstat site for performance evaluation

VoIP			Non-VoIP		
VoIP traffic traces	Size (MB)	Duration (seconds)	Non-VoIP traffic traces	Size (MB)	Duration
Google hangouts	12	3m21s	Online TV	36.8	3m2s
Facebook messenger	5.38	2m46s	Torrent	109	3m40s
Yahoo messenger	0.56	2m6s	Yahoo text chat	0.55	3m52s
Skype 7.2.2	4.88	5m	Online gaming	3m	9m5s
Viber	1.04	1m42s	Youtube	7.55	1m39s
Non-VoIP			Antivirus update	1.85	1m20s
Download manager/FTP	65	5min	Mixed Non VoIP	46	13m39s
Web Browsing	2.37	2m52s	Mixed VoIP and Non VoIP	9.28	5min

Table 7: Own captured VoIP and non-VoIP traffic traces for performance evaluation

5.3 Accuracy

We evaluated our system for accuracy. We considered the typical parameters used for measuring accuracy. These parameters are

- DR (Detection Rate): How many VoIP flows are correctly identified?
- FPR(False Positive Rate): Measure of flows incorrectly identified as VoIP
- TP (True positive): Measure of flows correctly identified as VoIP.
- FN(False Negative): Measure of flows that are incorrectly identified as Non-VoIP
- TN(True Negative): Measure of flow correctly identified as Non VoIP.

We calculated the DR and FP for different traces obtained from tstat, wireshark site and own VoIP and Non VoIP setups.

The accuracy is calculated by the expression

$$\text{Accuracy (DR)} = \frac{TP}{TP+FN} \times 100\% \quad (\text{Eq. 1})$$

$$\text{FPR} = \frac{FP}{FP+TN} \times 100\% \quad (\text{Eq. 2})$$

Total flows shows the total number flows in given data set. As discussed earlier, the system can only identify flow as VoIP or Non-VoIP if it is of duration equalvalent or above than 5 seconds or of 100 packets. In the data set of codec G729, 5 flows are detected but 2 of them has duration of beyond 5seconds. The system correctly identify it a VoIP

flow. In Skype dataset, out of 48 flows only 2 are beyond 5 seconds. Table 8 and 9 shows the accuracy and efficiency of the proposed system for rest of datasets.

5.4 Efficiency

We evaluated system efficiency in terms Average numbers of packets processed by our system per second and execution time. The average VoIP detection time for Voice traffic is less than 7 seconds.

Trace	Codec	Total Flows	TP	FP	Accuracy (DR)	FPR	Avg. packets processed/sec	Execution Time
E2E-140606-1	G729	5	2	0	100%	0.0%	22550.25	4sec
E2E-140606-1	iLBC	3	2	0	100%	0.0%	33391.66	3sec
	iSAC	2	2	0	100%	0.0%	24591.00	3sec
SkypeOut-260906-tcp	G729	4	2	0	100%	0.0%	22831.50	4sec
SkypeOut-260906-udp	G729	4	2	0	100%	0.0%	18468.80	5sec
Internet-E2X-29		20314	43	22	66%	33.8%	32301.32	1m15sec
Accuracy on tstat traces					94.33%	5.63%		

Table 8: Accuracy and efficiency w.r.t tstat traffic traces

VoIP Applications tested	Total flows	TP	FP	Accuracy	FPR	Average packets processed	Execution time
Google hangouts	2	2	0	100%	0%	15200	1sec
Facebook messenger	4	2	0	100%	0%	4104.0	1sec
Yahoo messenger	13	2	0	100%	0%	5200	1sec
Skype 7.2.2	48	2	0	100%	0%	32964.0	1sec
Viber	2	2	0	100%	0%	7322.0	1sec

Table 9: Accuracy and efficiency for own captured VoIP traffic traces

5.5 Scalability

We tested most familiar VoIP applications and detected VoIP traffic traces with high accuracy and efficiency. The proposed solution is generic and hence can detect VoIP flows regardless of application, protocol, codec used and security mechanism. The system can be implemented at one-way or two way network interface. Our system is only specific to VoIP detection so it has better results than other P2P traffic classifiers. So our system is scalable and practically implementable at telecommunication authorities or ISPs gateway with powerful servers and optimized and efficient programming implementation for realtime VoIP calls detection.

6 Conclusion and Future Work

In this paper we purposed a joint port and statistical analysis-based hybrid approach to detect encrypted, un-encrypted and tunneled VoIP and Non VoIP flows. We tested most common VoIP and non-VoIP applications and services and evaluated our system for accuracy, efficiency and scalability. Result shows that our system can detect VoIP flow with an accuracy of 97.165%. It is useless to detect VoIP flows after the communication has ended. Despite of calculating statistical values for the whole communication we focused on sliding window approach. Our system calculates statistical parameters for 5 seconds of the flow or only first 100 packets are analyzed to get threshold values. Our system can successfully detect VoIP within 6 seconds of communication. The proposed system is

generic, fast, and practically implementable which can be used to detect VoIP flows generated by any VoIP application. It can maintain validity when existing VoIP applications are updated or new ones admitted. It is best choice for ISPs, telecommunication authorities and law enforcement agencies to prioritize, block and for surveillance of VoIP traffic.

References

1. Leung, C.-M. and Y.-Y. Chan. *Network forensic on encrypted peer-to-peer voip traffics and the detection, blocking, and prioritization of skype traffics*. in *Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2007. WETICE 2007. 16th IEEE International Workshops on. 2007. IEEE.
2. Renals, P. and G.A. Jacoby. *Blocking skype through deep packet inspection*. in *System Sciences*, 2009. HICSS'09. 42nd Hawaii International Conference on. 2009. IEEE.
3. Risso, F.G.O., et al., *Lightweight, payload-based traffic classification: An experimental evaluation*. 2008.
4. Lu, F., X.-L. Liu, and Z.-N. Ma. *Research on the characteristics and blocking realization of Skype protocol*. in *Electrical and Control Engineering (ICECE)*, 2010 International Conference on. 2010. IEEE.
5. Ehlert, S., et al., *Analysis and signature of Skype VoIP session traffic*. 4th IASTED International, 2006.
6. Baset, S.A. and H. Schulzrinne, *An analysis of the skype peer-to-peer internet telephony protocol*. arXiv preprint cs/0412017, 2004.
7. Anwar, U., G. Shabbir, and M.A. Ali, *Data Analysis and Summarization to Detect Illegal VOIP Traffic with Call Detail Records*. International Journal of Computer Applications, 2014. **89**(8): p. 1-7.
8. Lin, Y.-D., et al., *Application classification using packet size distribution and port association*. Journal of Network and Computer Applications, 2009. **32**(5): p. 1023-1030.
9. Zuev, D. and A.W. Moore, *Traffic classification using a statistical approach*, in *Passive and Active Network Measurement*. 2005, Springer. p. 321-324.
10. Yildirim, T. and P. Radcliffe. *A framework for tunneled traffic analysis*. in *Advanced Communication Technology (ICACT)*, 2010 The 12th International Conference on. 2010. IEEE.
11. Khan, F.I.U.A., *A generic technique for voice over internet protocol (VoIP) traffic detection*. IJCSNS, 2008. **8**(2): p. 52.
12. Freire, E.P., A. Ziviani, and R.M. Salles, *Detecting VoIP calls hidden in web traffic*. Network and Service Management, IEEE Transactions on, 2008. **5**(4): p. 204-214.
13. Freire, E.P., A. Ziviani, and R.M. Salles. *Detecting skype flows in web traffic*. in *Network Operations and Management Symposium*, 2008. NOMS 2008. IEEE. 2008. IEEE.
14. Crotti, M., et al. *A statistical approach to IP-level classification of network traffic*. in *Communications*, 2006. ICC'06. IEEE International Conference on. 2006. IEEE.
15. Okabe, T., T. Kitamura, and T. Shizuno. *Statistical traffic identification method based on flow-level behavior for fair VoIP service*. in *VoIP Management and Security*, 2006. 1st IEEE Workshop on. 2006. IEEE.
16. Piskac, P. and J. Novotny, *Using of time characteristics in data flow for traffic classification*, in *Managing the Dynamics of Networks and Services*. 2011, Springer. p. 173-176.
17. Korczynski, M. and A. Duda. *Classifying service flows in the encrypted Skype traffic*. in *Communications (ICC)*, 2012 IEEE International Conference on. 2012. IEEE.
18. Zander, S., T. Nguyen, and G. Armitage. *Automated traffic classification and application identification using machine learning*. in *Local Computer Networks*, 2005. 30th Anniversary. The IEEE Conference on. 2005. IEEE.
19. Nguyen, T.T. and G. Armitage, *A survey of techniques for internet traffic classification using machine learning*. Communications Surveys & Tutorials, IEEE, 2008. **10**(4): p. 56-76.

20. Alshammari, R. and A.N. Zincir-Heywood, *How Robust Can a Machine Learning Approach Be for Classifying Encrypted VoIP?* Journal of Network and Systems Management, 2014: p. 1-40.
21. Alshammari, R. and A.N. Zincir-Heywood, *Identification of VoIP encrypted traffic using a machine learning approach.* Journal of King Saud University-Computer and Information Sciences, 2015.
22. McGregor, A., et al., *Flow clustering using machine learning techniques*, in *Passive and Active Network Measurement*. 2004, Springer. p. 205-214.
23. Gómez Sena, G. and P. Belzarena. *Early traffic classification using support vector machines.* in *Proceedings of the 5th International Latin American Networking Conference*. 2009. ACM.
24. Gowsalya, R.A. and S.M.J. Amali, *SVM Based Network Traffic Classification Using Correlation Information*. Networking and Communication Engineering, 2014. **6**(5): p. 188-192.
25. Alshammari, R. and A.N. Zincir-Heywood, *Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?* Computer networks, 2011. **55**(6): p. 1326-1350.
26. Alshammari, R. and A.N. Zincir-Heywood. *An investigation on the identification of VoIP traffic: Case study on Gtalk and Skype.* in *Network and Service Management (CNSM), 2010 International Conference on*. 2010. IEEE.
27. Do, L.H. and P. Branch, *Real time VoIP traffic classification*. Techni-cal Report 090914AIR].[S. 1.]: CAIA, 2009.
28. Adami, D., et al., *Skype-Hunter: A real-time system for the detection and classification of Skype traffic*. International Journal of Communication Systems, 2012. **25**(3): p. 386-403.
29. Adami, D., et al., *A real-time algorithm for skype traffic detection and classification*, in *Smart Spaces and Next Generation Wired/Wireless Networking*. 2009, Springer. p. 168-179.
30. Birke, R., et al., *Experiences of VoIP traffic monitoring in a commercial ISP*. International Journal of Network Management, 2010. **20**(5): p. 339-359.
31. Birke, R., et al. *Understanding VoIP from backbone measurements.* in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications*. IEEE. 2007. IEEE.
32. IPSec, http://en.wikipedia.org/wiki/IPsec#Transport_mode
33. Skype Traces, <http://tstat.tlc.polito.it/traces-skype.shtml>
34. Sample VoIP and non-VoIP traffic traces, <http://wiki.wireshark.org/SampleCaptures>

Comparative Study of Similarity Measures in Link Prediction Using Facebook Data

Faiza Khan, Department of Computer Science, University of Karachi

Madiha Fatima, Department of Computer Science, University of Karachi

Usman Tariq Alvi, Department of Computer Science, University of Karachi

Tahseen Jilani, Department of Computer Science, University of Karachi

Ubaida Fatima, Department of Mathematics, NED University of Engineering and Technology

Abstract

Social networks are growing like a giant for the duration of several past years. This emergence has made a magneto effect on researchers of network analytics field. In this article, we are going to examine Link Prediction in Social Network. It is a problem that guesstimates the probability of existence of future links between any two particular nodes. In the following article, we will use four different similarity based proximity measures namely: Common Neighbor; Jaccard Index; Salton Index and Preferential Attachment. We will experiment these proximity measures on Facebook data that has been collected from SNAP (Stanford Network Analysis Project) and find out AUC (Area Under the receiver operating Characteristic curve) to analyze accuracy.

KEY TERMS:

Social Networks Analysis, Link Prediction, Proximity Measures, Common Neighbors, Jaccard index.

INTRODUCTION

In the recent past years, hastily emergence of networks is the key reason behind the development of network analytics field. Analysis can be carried out in different dimensions like social networks, metabolic structure of biological networks, commodity distribution networks which can be termed as technological networks, information networks etc.

During some time, an enormous research has been made on real world complex networks. According to current research mostly real networks possesses; high clustering coefficient, undersized diameter and, degree distribution that is followed by power law [1]. Here in this article, we will discuss concerning to social networks. We can define social network as a media or interface where set or group of people interact with each other having some kind of relationship among them.

Link prediction is basically finding the association between two nodes that have higher probability of collaboration (interaction) in future. Predicting links is useful in variety of fields. In business it analyzes and improves communication with your customers. For security reasons it is used by secret intelligence agencies to track the criminals. In short for several reasons it is used in various fields such as information retrieval, medical, network analysis, recommendation systems etc.

Lu and Zhou in October 2010 provided an overall survey of link prediction problem. They explain that Link prediction technique can also be used for finding the spurious links, and evolution mechanism of network. Similarity based indices is divided in three categories; which are local indices, global indices and quasi local indices. They suggested that the accuracy of the link prediction algorithms can be proofed by the two methods: Area Under the receiver operating Characteristic curve (AUC) and Precision. According to their research applications of link prediction can be categorized into three divisions: Reconstruction of networks; Classification of partially labeled networks; Evolution of network evolving measures [2].

Bliss, Frank, Danforth and Dodds in 2013 observed that link prediction strategy can be divided into three categories similarity based strategies, maximum likelihood algorithms and probabilistic models. They put their research on similarity based indices which have two major classes topological and node based attributes. In their research, a linear model was proposed for combining similarity neighborhood measures. For this purpose Covariance Matrix Adaptation Evolution Strategy (CMAES) was used for finding the coefficients which optimize the correct prediction of future links [3].

Liben-Nowell and Kleinberg in 2004 proposed different approaches which are based on different proximity measures to evaluate prediction of link in a network. They used the co-authorship network and concluded that by using singly-handled network topology we can predict the future links [4].

Chen, Lou, Zhang, Zhou and Shang in 2011 suggested that identification of influential nodes that lead to widely spreading of a network is highly significant. Metrics like closeness centrality and betweenness centrality can be used for this purpose. But when the network is huge they cannot be applied due to computational complexity. They proposed the semi local centrality measure that act as a substitution for the low relative degree centrality and other measures. They used Susceptible Infected Recovered (SIR) model to evaluate spreading rate and influential nodes [5].

Newman in 2001 evaluates that in collaboration network two scientists are said to be connected, if they have minimum one research paper together. He also exemplifies that scientist collaboration's probability raise when the number of scientist they have in common increases. Also, acquiring of new collaborators depends on past number of one's collaborators. [6]

Gao, Musial, Cooper and Tsoka in 2014 examined correlation among different metrics of the networks. Also, he investigates the accuracy of some prediction techniques. They gathered some time stamp social networks and then applied some link prediction techniques on these networks. They put out the conclusion that there are two types of networks: prediction friendly networks, prediction unfriendly networks. [7]

DATASET:

As Facebook emerges very fast and strengthen its roots in every aspect of life so we decided to take Facebook dataset. We try to examine that by using this dataset on our algorithms what results are obtained. Dataset of

Facebook is openly available on **SNAP** (Stanford Network Analysis Project)[8]. In this dataset we have around 4000 nodes or individual user Id's and around 88,000 links between those nodes with undirected in nature.

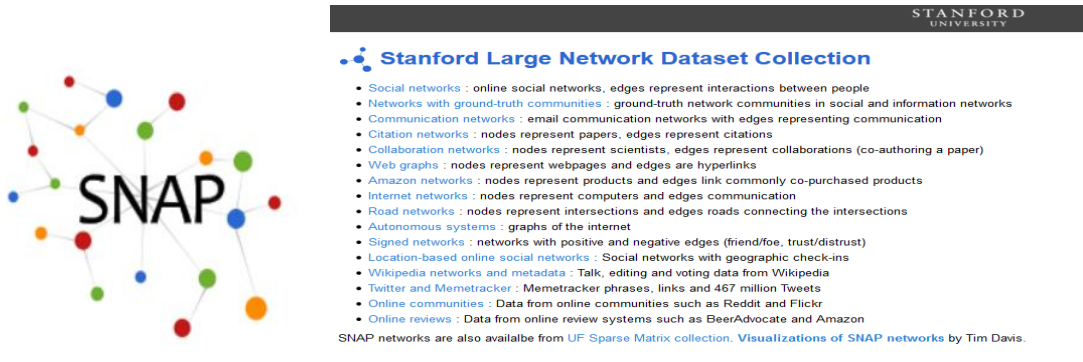


Figure. 1. Snapshot of source website from where dataset of Facebook is retrieved.

METHODOLOGIES:

The principal behind Node neighborhood methods is that consider a scenario where A and B are two students, if there are any friend common between A and B it means there is probability that in future A and B also becomes friends. Greater the no. of common neighbors greater the probability of association between two nodes. We are going to apply 4 types of node neighborhood measures to predict that in future how the networks looks due to new bonds that are formed between various nodes.

❖ *Common Neighbor:-*

Common neighbor is a simplest measure where we are considering the common neighbors of node x and y using the intersection property. [8]

$$\text{Score}(x, y) = |N(x) \cap N(y)| \quad (1)$$

Using the adjacency matrix A we are calculating this measure. We can also say that

$$\text{Score}(x, y) = A^2(x, y) \quad (2)$$

It means that all the common neighbors are having path length of 2. Newman [6] shows that the probability of scientists collaborating increases with the number of other collaborators they have in common.

❖ *Jaccard's coefficient:-*

This measure is normalized measure of common neighbors. We are finding the ratio of no. of common neighbors with the total no. of neighbors between two nodes.

$$\text{Score}(x, y) = \frac{|N(x) \cap N(y)|}{|N(x) \cup N(y)|} \quad (3)$$

❖ *Salton index:-*

In this measure we are finding the score by determining the ratio between the no. of common neighbor relative to the geometric mean of two nodes (square root of the product between the degrees of two nodes).[10]

$$\text{Score}(x, y) = \frac{|N(x) \cap N(y)|}{\sqrt{|x| * |y|}} \quad (4)$$

❖ *Preferential attachment:-*

In some cases it is observed that the likelihood of future association(link) to be occur between two nodes is directly proportional to the degree of the nodes [6] .This measure could be calculated as a product of degree of node x and y.

$$\text{Score}(x, y) = |x| * |y| \quad (5)$$

The Algorithms of above mentioned proximity measures are shown below which are experimented on the Facebook dataset that we have taken from SNAP.

Algorithm # 1: Algorithm for Common Neighbor measure

```

Function[]= COMMON_NEIGHBOR(AM)

for i=1:r-1
  for k=i+1:r
    S ← 0
    for j=1:c
      if AM(i,j) == 1 AND AM(k,j)==1
        S ← S + 1;
      end_if
    end_for
  end_for
end_for

```

Algorithm # 2: Algorithm for Jaccard Index measure

```

Function[]=JACCARD_INDEX(AM)
for i=1:r-1
  for k=i+1:r
    S ← 0
    for j=1:c
      if AM(i,j) == 1 AND AM(k,j)==1
        S ← S + 1;
      end_if
    end_for
    S ← S/c;
  end_for
end_for

```

Algorithm # 3: Algorithm for Salton Index measure

```

Function[]=SALTON_INDEX(AM)
for i=1:r-1
  for k=i+1:r
    S ← 0
    for j=1:c
      if AM(i,j) == 1 AND AM(k,j)==1
        S ← S + 1;
      end_if
    end_for
    sq ←sqrt(da * db);
    S ← S / sq;
  end_for
end_for

```

Algorithm # 4: Algorithm for Preferential Attachment measure

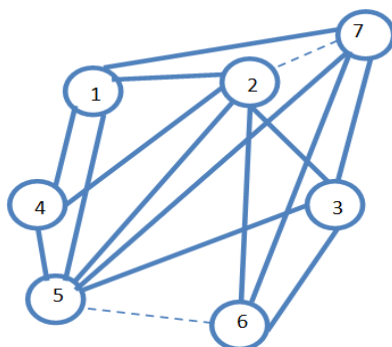
```

Function[]=PREFERENTIAL_ATTACHMENT(AM)
for i=1:r-1
  for k=i+1:r
    S ← 0
    for j=1:c
      if AM(i,j) == 1 AND AM(k,j)==1
        S ← S + 1;
      end_if
    S ← da * db
  end_for
end_for
end_for

```

To understand the results of various neighborhood based local similarity measures let's consider some examples of small networks that how they work on our algorithms and comparing manually solved results with the computational output. Let's assume 2 networks namely network A & B respectively.

Network A is an undirected network of a friends group of any social circle consisting 7 nodes.



Total no. Of nodes=7
Total no. Of edges/links=16
Probe links= {(2, 7), (5, 6)}
Non-existing links= {(1, 3), (1, 6), (3, 4), (4, 6), (4, 7)}

Figure. 2. Visualization of Network A consisting 7 nodes and 16 links.

Now on this network by performing all the four similarity measures discussed above we will analyze the results of AUC and score measures obtained computationally and manually.

TABLE 1. The scores obtained from common neighbor measure for fig 2. Each calculation is done by using (1). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	2	2
1,3	3	3
1,4	2	2
1,5	3	3
1,6	2	2
1,7	1	1
2,3	2	2
2,4	2	2
2,5	3	3
2,6	1	1
2,7	4	4
3,4	2	2
3,5	2	2
3,6	2	2
3,7	2	2
4,5	2	2
4,6	1	1
4,7	2	2
5,6	3	3
5,7	2	2
6,7	1	1

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.85	0.8500

TABLE 3. The scores obtained from Salton index measure for fig 2. Each calculation is done by using (4). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	0.45	0.4472
1,3	0.75	0.7500
1,4	0.6	0.5774
1,5	0.7	0.6708
1,6	0.6	0.5774
1,7	0.25	0.2500
2,3	0.45	0.4472
2,4	0.5	0.5164
2,5	0.6	0.6000
2,6	0.3	0.2582
2,7	0.9	0.8944
3,4	0.6	0.5774
3,5	0.45	0.4472
3,6	0.6	0.5774
3,7	0.5	0.5000
4,5	0.5	0.5164
4,6	0.3	0.3333
4,7	0.6	0.5774
5,6	0.8	0.7746
5,7	0.45	0.4472
6,7	0.3	0.2887

TABLE 2. The scores obtained from Jaccard index measure for fig 2. Each calculation is done by using (3). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	0.3	0.2857
1,3	0.4	0.4286
1,4	0.3	0.2857
1,5	0.4	0.4286
1,6	0.3	0.2857
1,7	0.1	0.1429
2,3	0.3	0.2857
2,4	0.3	0.2857
2,5	0.4	0.4286
2,6	0.1	0.1429
2,7	0.6	0.5714
3,4	0.3	0.2857
3,5	0.3	0.2857
3,6	0.3	0.2857
3,7	0.3	0.2857
4,5	0.3	0.2857
4,6	0.1	0.1429
4,7	0.3	0.2857
5,6	0.4	0.4286
5,7	0.3	0.2857
6,7	0.1	0.1429

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.85	0.8500

TABLE 4. The scores obtained from Preferential Attachment measure for fig 2. Each calculation is done by using (5). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	20	20
1,3	16	16
1,4	12	12
1,5	20	20
1,6	12	12
1,7	16	16
2,3	20	20
2,4	15	15
2,5	25	25
2,6	15	15
2,7	20	20
3,4	12	12
3,5	20	20
3,6	12	12
3,7	16	16
4,5	15	15
4,6	9	9
4,7	12	12
5,6	15	15
5,7	20	20
6,7	12	12

AUC MEASURE	
MANUAL	COMPUTATIONAL
1	0.999

AUC MEASURE	
MANUAL	COMPUTATIONAL
1	0.999

By observing the results of scores of all four similarity measures that we have experimented in this small network 'A' we can say that algorithm gives almost same results for AUC measures and for Score measures solved manually and through computation. This shows that our computation is correct for any input network to determine its scores and accuracy that how much the results obtained are near to accurate results.

In previous network we have 7 nodes so now we are considering another example consisting 10 nodes. This is also an undirected network namely 'B'. Now we will check all the four measures results on this network of 10 people and 21 links that keep them in contact with each other.

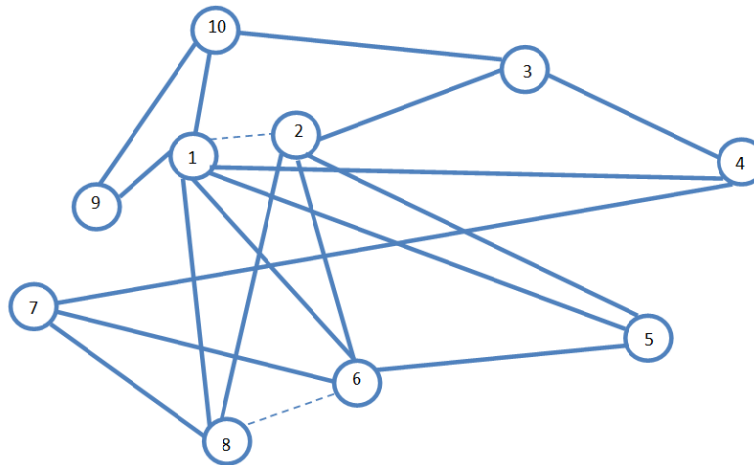


Figure. 3. Visualization of Network B consisting 10 nodes and 19 links between them.

Total no. Of nodes= 10

Total no. Of edges/links= 19

Probe links= {(1, 2), (6, 8)}

Non-existing /missing

links= {(1,3),(1,7),(2,4),(2,7),(2,9),(2,10),(3,5),(3,6),(3,7),(3,8),(3,9),(4,5),(4,6),(4,8),(4,9),(4,10),(5,7),(5,8),(5,9),(5,10),(6,9),(6,10),(7,9),(7,10),(8,9),(8,10)}

TABLE 5. The scores obtained from common neighbor measure for fig 3. Each calculation is done by using (1). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	3	3
1,3	2	2
1,4	0	0
1,5	1	1
1,6	1	1
1,7	3	3
1,8	0	0
1,9	1	1
1,10	1	1

TABLE 6. The scores obtained from Jaccard index measure for fig 3. Each calculation is done by using (3). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	0.3	0.3000
1,3	0.2	0.2000
1,4	0	0
1,5	0.1	0.1000
1,6	0.1	0.1000
1,7	0.3	0.3000
1,8	0	0
1,9	0.1	0.1000
1,10	0.1	0.1000

2,3	0	0
2,4	1	1
2,5	1	1
2,6	1	1
2,7	2	2
2,8	0	0
2,9	0	0
2,10	1	1
3,4	0	0
3,5	1	1
3,6	1	1
3,7	1	1
3,8	1	1
3,9	1	1
3,10	0	0
4,5	1	1
4,6	2	2
4,7	0	0
4,8	2	2
4,9	1	1
4,10	2	2
5,6	2	2
5,7	1	1
5,8	2	2
5,9	1	1
5,10	1	1
6,7	0	0
6,8	3	3
6,9	1	1
6,10	1	1
7,8	0	0
7,9	0	0
7,10	0	0
8,9	1	1
8,10	1	1
9,10	1	1

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.94	0.9423

TABLE 7. The scores obtained from Salton index measure for fig 3. Each calculation is done by using (4). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	0.6	0.6124
1,3	0.5	0.4714
1,4	0	0
1,5	0.2	0.2357
1,6	0.2	0.2041
1,7	0.7	0.7071
1,8	0	0
1,9	0.3	0.2887
1,10	0.2	0.2357
2,3	0	0
2,4	0.3	0.2887
2,5	0.3	0.2887
2,6	0.25	0.2500
2,7	0.3	0.3333
2,8	0.3	0.3333

2,3	0	0
2,4	0.1	0.1000
2,5	0.1	0.1000
2,6	0.1	0.1000
2,7	0.2	0.2000
2,8	0	0
2,9	0	0
2,10	0.1	0.1000
3,4	0	0
3,5	0.1	0.1000
3,6	0.1	0.1000
3,7	0.1	0.1000
3,8	0.1	0.1000
3,9	0.1	0.1000
3,10	0	0
4,5	0.1	0.1000
4,6	0.2	0.2000
4,7	0	0
4,8	0.2	0.2000
4,9	0.1	0.1000
4,10	0.2	0.2000
5,6	0.2	0.2000
5,7	0.1	0.1000
5,8	0.2	0.2000
5,9	0.1	0.1000
5,10	0.1	0.1000
6,7	0	0
6,8	0.3	0.3000
6,9	0.1	0.1000
6,10	0.1	0.1000
7,8	0	0
7,9	0	0
7,10	0	0
8,9	0.1	0.1000
8,10	0.1	0.1000
9,10	0.1	0.1000

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.94	0.9423

TABLE 8. The scores obtained from Preferential Attachment measure for fig 3. Each calculation is done by using (5). Accuracy is also shown in end for the corresponding measures.

NODES	SCORE MEASURE	
	MANUAL	COMPUTATIONAL
1,2	0.6	0.6124
1,3	0.5	0.4714
1,4	0	0
1,5	0.2	0.2357
1,6	0.2	0.2041
1,7	0.7	0.7071
1,8	0	0
1,9	0.3	0.2887
1,10	0.2	0.2357
2,3	0	0
2,4	0.3	0.2887
2,5	0.3	0.2887
2,6	0.25	0.2500
2,7	0.3	0.3333
2,8	0.3	0.3333

2,9	0.4	0.4082
2,10	0	0
3,4	0	0
3,5	0.3	0.3333
3,6	0.3	0.2887
3,7	0.3	0.3333
3,8	0.3	0.3333
3,9	0.4	0.4082
3,10	0	0
4,5	0.3	0.3333
4,6	0.6	0.5774
4,7	0	0
4,8	0.7	0.6667
4,9	0.4	0.4082
4,10	0.7	0.6667
5,6	0.6	0.5774
5,7	0.3	0.3333
5,8	0.7	0.6667
5,9	0.4	0.4082
5,10	0.3	0.3333
6,7	0	0
6,8	0.9	0.8660
6,9	0.35	0.3536
6,10	0.3	0.2887
7,8	0	0
7,9	0	0
7,10	0	0
8,9	0.4	0.4082
8,10	0.3	0.3333
9,10	0.4	0.4082

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.942	0.999

2,9	8	8
2,10	12	12
3,4	9	9
3,5	9	9
3,6	12	12
3,7	9	9
3,8	9	9
3,9	6	6
3,10	9	9
4,5	9	9
4,6	12	12
4,7	9	9
4,8	9	9
4,9	6	6
4,10	9	9
5,6	12	12
5,7	9	9
5,8	9	9
5,9	6	6
5,10	9	9
6,7	12	12
6,8	12	12
6,9	8	8
6,10	12	12
7,8	9	9
7,9	6	6
7,10	9	9
8,9	6	6
8,10	9	9
9,10	6	6

AUC MEASURE	
MANUAL	COMPUTATIONAL
0.82	0.8200

In the above table results are computed manually by using equations mention for proximity measures. For example in fig 3 node 1 and 2 have 3 friends common that's why the intersection taken for adjacency matrix is 3 for the following node as described in (1). Similarly for Jaccard index measure the node 1&2 has 3 common friends and total friends of 1 and 2 are 10. So using (3) $3/10 = 0.3$. For Salton index we have used (4) $3/\sqrt{24}=0.6124$. Similarly by using (5) we have $6*4=24$ results. So it is determined that we have almost accurate results for any network data. We have shown in above tables the algorithm's computation results that have mentioned above. AUC [8] has been calculated by the formula

$$\frac{(N' - N'')}{N} \quad (6)$$

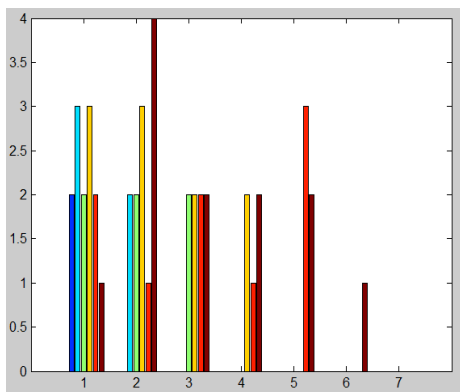


Figure. 4. Histogram showing the computational results of table 1.

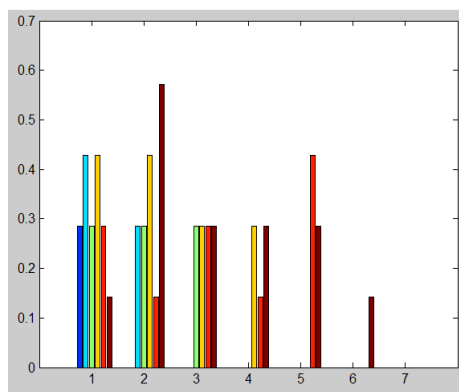


Figure. 5. Histogram showing the computational results of table 2.

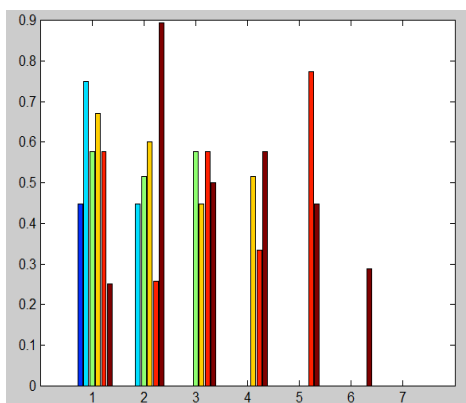


Figure. 6. Histogram showing the computational results of table 3.

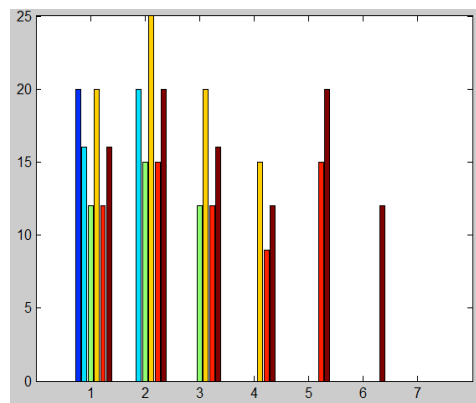


Figure. 7. Histogram showing the computational results of table 4

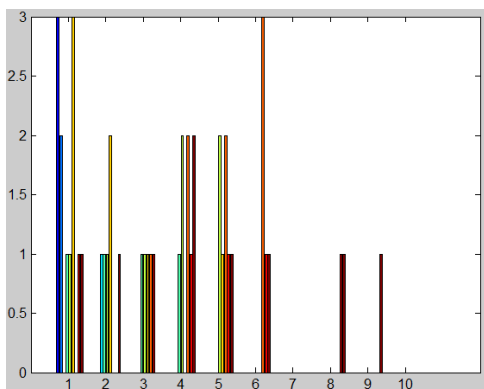


Figure. 7. Histogram showing the computational results of table 5.

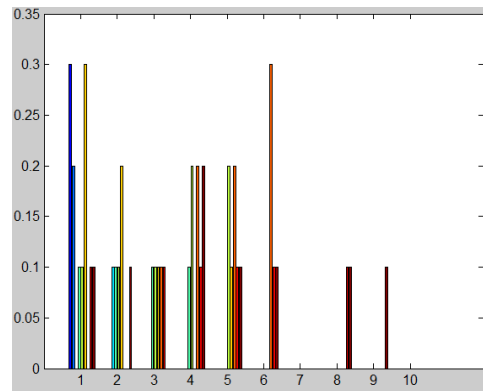


Figure. 8. Histogram showing the computational results of table 6.

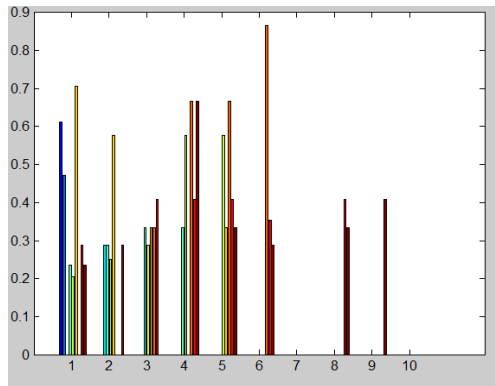


Figure. 9. Histogram showing the computational results of table 7.

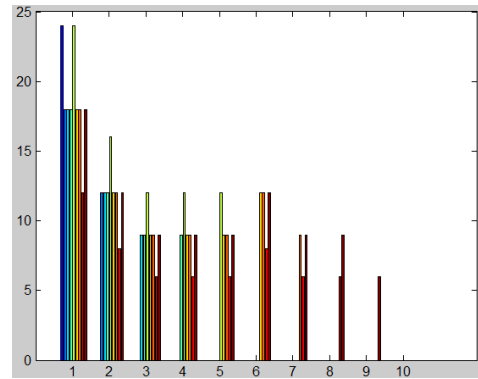


Figure. 10. Histogram showing the computational results of table 8.

RESULTS:

Above explanation is based on random dataset, network A and B, now we are taking our Facebook Dataset as define in dataset in introduction part, due to big data and limited resources for its execution purpose we take biased records and divide 4000 nodes to 1800 to get its result in for calculation purpose[8].

Now we have our dataset first of all we divide our data into two parts one is training set and other is test set with a ratio of 60:40[8]. Training set comprise of our original or you can say that existing links. And test set is of investigating links, on which we calculate our predictions.

Steps:

1. Divide our data in train and test set.
2. Apply Algorithms defined above on our training set. And calculate results.
3. Calculate AUC[8] with the input arguments of algorithms results and test set.
4. Calculate AUC. Set minimum threshold of AUC[8] to 0.5. If results of AUC is greater than 0.5 than it shows good result hence indicating that particular node have high probability / prediction to be connected in future.

Our results after running above steps on all four algorithms are approx. to 0.5 AUC. Due to minimum selection of our dataset from 4000 to 1800, to minimize execution time, our results are not so good but not worst either.

TABLE 9:- AUC of Facebook dataset

Common Neighbor	0.5000
Jaccard Index	0.4958
Salton Index	0.4990
Preferential Attachment	0.4700

CONCLUSION:

Various techniques have been designed by the number of scientist to solve the link prediction problem. Link prediction problem can be broadly distributed in three categories namely: similarity based indices, maximum likelihood based indices, and probability based indices [2]. In our research we focused only on similarity base measures. We used four similarity based proximity measures namely: Common Neighbor; Jaccard Index; Salton Index and Preferential Attachment. We experimented these proximity measures on Facebook data that had been collected from SNAP (Stanford Network Analysis Project) and find out AUC (Area Under the receiver operating Characteristic curve). In the light of above research, by observing the results of all four measures we can conclude that common neighbor has predicted finest among rest proximity measures. Future work is that one can apply different other measures to improve the AUC results.

ACKNOWLEDGEMENT

First and foremost, we would like to thanks Almighty Allah. We are also thankful to our supervisor Dr. Tahseen Jilani and Ms. Ubaida Fatima for their cooperation and guidance during our research work.

REFERENCES:

- [1] Newman, M. E. (2003).The structure and function of complex networks.
- [2] Z. Lu, B. Savas, W. Tang, I. Dhillon, Supervised link prediction using multiple sources, in: 2010 IEEE 10th International Conference on Data Mining (ICDM),IEEE, 2010, pp. 923–928.
- [3]An evolutionary algorithm approach to link prediction in dynamic social networks Catherine A. Bliss, Morgan R. Frank, Christopher M. Danforth, Peter Sheridan Dodds.
- [4] The Link Prediction Problem for Social Networks, David Liben-Nowell, Jon Kleinberg.
- [5]Identifying influential nodes in complex networks, Duanbing Chen, Linyuan Lü, Ming-Sheng Shang, Yi-Cheng Zhang, Tao Zhou.
- [6] M. E. J. Newman, Clustering and preferential attachment in growing networks Phys. Rev. E 64 (2001) 025102.
- [7]Fei Gao, Katarzyna Musial, Colin Cooper, and Sophia Tsoka, Link Prediction Methods and Their Accuracy for Different Social Networks and Network Metrics.
- [8] Linyuan Lu ,Tao Zhou , Link prediction in complex networks: A survey, March 2011.
- [9]G.Salton,M.McGill,IntroductiontoModernInformationRetrieval,1986.

Straight Line Delineation using Hough Transform on an Aerial Greenfield Imagery

Babawuro Usman and Bashir Yusuf Bichi

Department of Computer Science, Kano University of Science and Technology, Wudil

Abstract-Hough Transform which could be used to link straight lines has been practically employed using Matlab as a computing tool, to delineate the straight edges of Aerial Greenfield imagery boundaries that demarcate some cadastral features. The demarcation is of utmost importance as it shows the extent and limit of each piece of land which is very crucial in Cadastral Science. In this paper, with the help of this popular transform, we have been able to successfully detect the boundaries and delineate the lands. With further perfection, the employment of these digital image processing algorithms could provide better alternative method over the hitherto ways being used in Plane Surveys.

Keywords: Hough transform, Digital imagery, Straight line, delineation

I. INTRODUCTION

The Hough Transform (HT) was first proposed by Hough (Hough, 1962) [1]. It is considered a very powerful tool in straight line detection and edge linking [2][5]. Its main advantages are its insensitivity to noise and its capability to extract lines even in areas with pixel absence, pixel gaps. The standard HT proposed by Duda and Hart in 1972, has been widely applied for line extraction in natural scenes, while some of its variants have been used for features extraction purposes [3]. The classical HT is most commonly used for the detection of regular curves such as lines, circles, ellipses, etc. It requires that the desired features be specified in some parametric form. To detect straight lines using this method was presented by Duda and Hart. When many distributed points seem to be in the straight line, the original line can be traced along these points via the transform. One pixel in image space is represented as one straight line in parameter space. Many pixels that are supposed to be a straight line in parameter space are mapped to many lines in image space. Crossing point of these lines in parameter space is detected as one straight line segment in the image space.

In this paper, to delineate the straight edges of the Greenfield cadastral boundaries, HT has been used using Matlab as a computing tool. With the help of this popular transform, we have been able to detect the boundaries and delineate the lands. With further perfection, the employment of these digital image processing algorithms could provide alternative method over the hitherto ways used in Plane Surveying. The paper concludes as follows: section two contains the mathematical background; section three has the implementation; results and discussions in section four and finally conclusion of the paper in section five.

II. MATHEMATICAL BACKGROUND

Let's consider all the possible lines which can go through an image point (s, t) : $t = m s + c$. The parameters of all these lines form a straight line in the parameter space m, c . Both m and c can attain any value from $-\infty$ to $+\infty$.

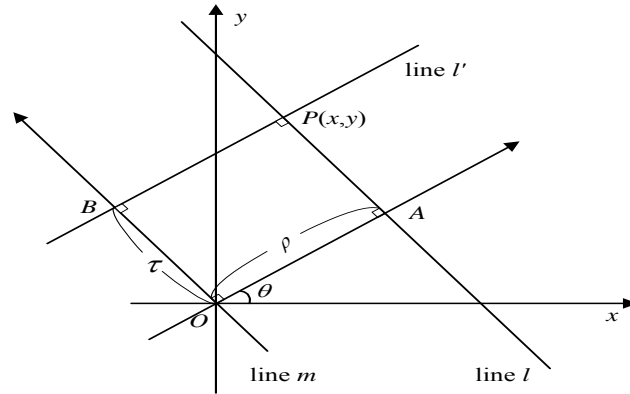


Fig.2.1 Hough transform for line detection

Hough transform [4, 1] for line detection yields an equation of a line for line l shown Fig.2.1

$$\rho = x \cos \theta + y \sin \theta \quad (2.00)$$

Where, $x = a + \rho \cos \theta$ and $y = b + \rho \sin \theta$

where ρ is the normal distance of the line l from the origin O passing through a feature point P(x,y) shown in Fig. 2.1 or equivalently, the distance of the line OA that is normal to the line l. θ represents the angle between the x-axis and the line OA, with $0 \leq \theta < 2\pi$ and $-\rho_{\max} \leq \rho \leq \rho_{\max}$. Since ρ is reversed whenever $\theta = 2\pi$, $0 \leq \theta < \pi$ and $-\rho_{\max} \leq \rho \leq \rho_{\max}$ are assumed, $\rho_{\max} = K/\sqrt{2}$ is measured from the center O of the image $K \times K$. Note that, the point A is the most nearest point from the origin, among all the points on line l. There are infinite number of lines which pass through a fixed pixel in an image plane, with each line represented by two parameters θ and ρ . Thus a single pixel in the image plane is mapped into an infinite number of points in the θ - ρ line parameter space.

III.IMPLEMENTATION OF THE TRANSFORM

Detection of the dominant line in the image plane is achieved by finding a peak in the accumulators of parameter arrays. Each of the straight lines passing through a fixed point in an image plane is mapped into a large number of discrete points (θ_n, ρ_{mn}) , $0 \leq n \leq N$, $-M \leq m \leq M$, on a periodic sinusoidal curve in the θ - ρ parameter space, where N and $(2M+1)$ represent the total numbers of quantized angle and distance cells, respectively. Note that θ_n is the nth uniformly quantized angle of θ in the bounded parameter space, for reduction of the computational complexity, and that ρ_{mn} denotes the quantized distance of ρ_n that corresponds to θ_n . The computational attractiveness of the Hough transform arises from sub-dividing the θ - ρ parameter space into so-called accumulator cells [5]. The transform is implemented by quantizing the Hough parameter space into accumulator cells. In the beginning, the accumulator cells are set to zero. As the algorithm runs, each (x_i, y_i) is transformed into a discretized (θ_n, ρ_{mn}) , and the accumulator cells that lie along this line are incremented. Resulting peaks in the accumulator array represent strong evidence that a corresponding straight line exists in the image.

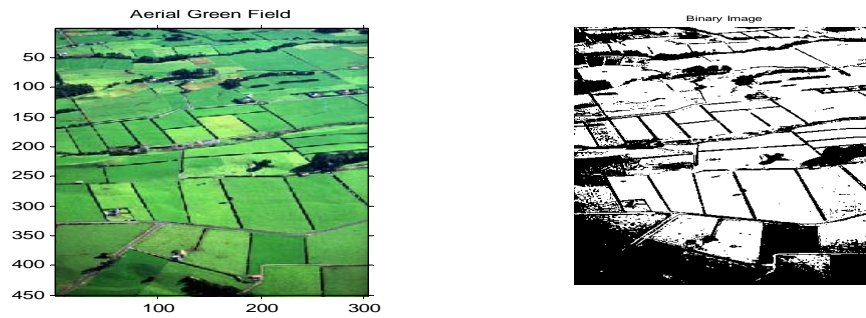


Fig.3.1 An image of aerial Greenfields and its Binary Image

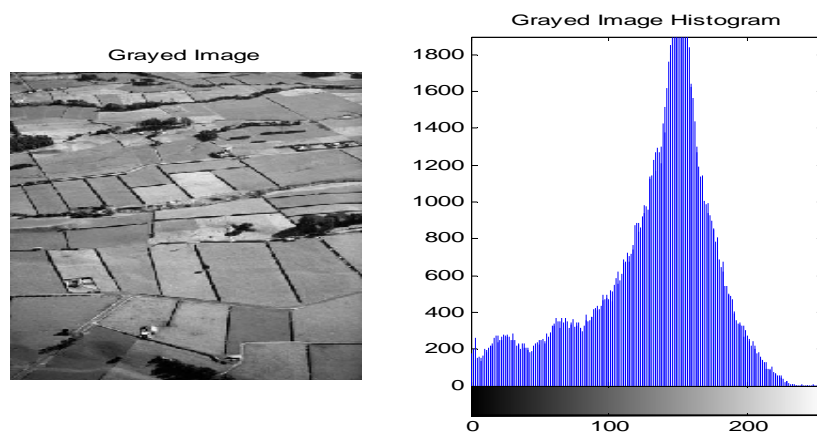


Fig.3.2 Gray image of the Greenfields and its Histogram

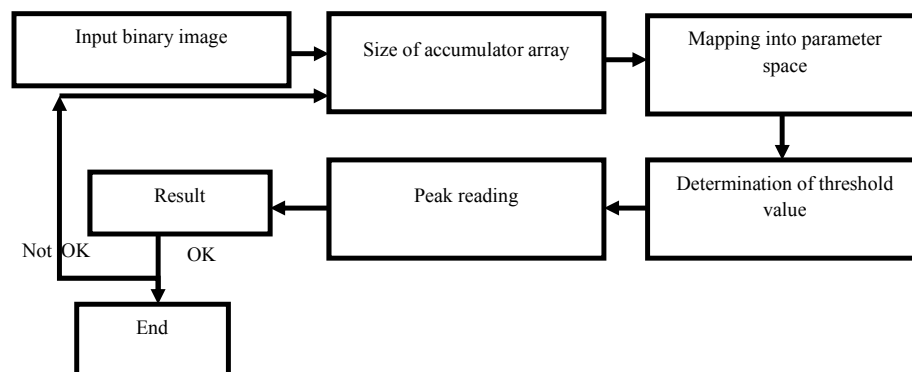


Fig.3.3 Flowchart of Hough transform procedure

IV.RESULTS AND DISCUSSIONS

Hough Transform divides the parameter space of the geometric primitive into cells, usually rectangular, by quantizing each dimension into a fixed number of intervals. Each datum point adds a

vote to every cell whose parameters are such that the primitive associated with that cell passes through the point. After all the points have been voted, the cells which have number of votes greater than a threshold are marked. For each such a cell, the associated geometric primitive is taken as a description of the points that voted for the cell, and this primitive is said to be extracted from the data. It is shown to be equivalent to template matching where the templates are defined by each of the cells in parameter space. Applying HT to the Aerial Greenfield image, Fig.3.1, we obtained Fig.4.1, Fig.4.2 and Fig.4.3 as the results.

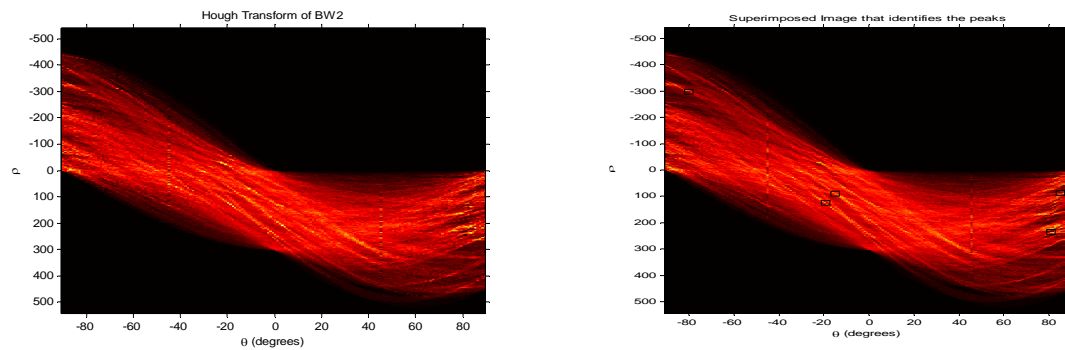


Fig.4.1 Hough transform and its peaks

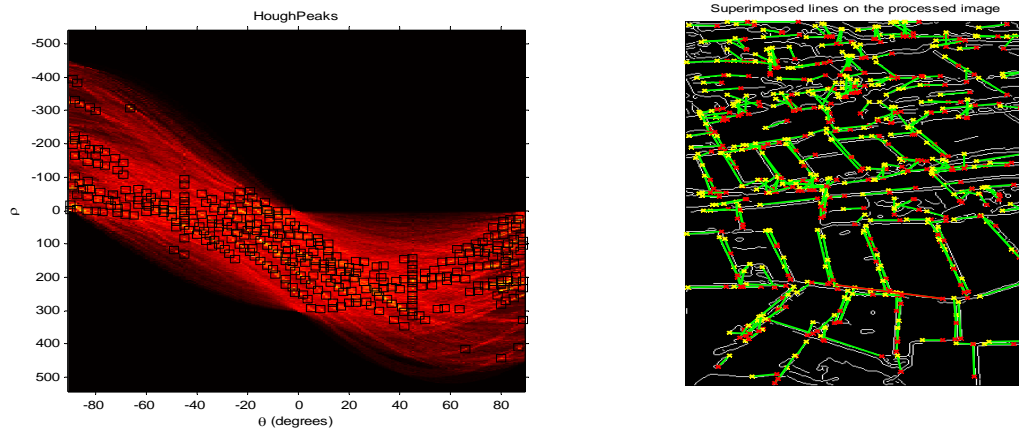


Fig.4.2 More peaks as the parameters are varied

Fig.4.3 Lines delineated in colors from an Aerial Green field image using Hough transform

V. CONCLUSION

To delineate the Greenfield Imagery straight line boundary edges, Hough transform has been applied to the imagery concerned. From the result, we noted that this transform, though there have been few omissions, detected and delineated the edges as straight lines. There are many opportunities and challenges in using HT processing for extracting and delineating cadastral features. It is an area of growing importance both locally and globally. More attention from the image processing community needs to be directed toward studying extracting and delineating cadastral features, as a result of their

socio economic and environmental values. In our work, though boundaries of the farmlands are extracted and delineated clearly and within acceptable limits, there are some boundaries that are not well captured. These omissions could be perfected with further improvements on the algorithms.

ACKNOWLEDGEMENT

We express gratitude to Kano University of Science and Technology, KUST, Wudil, for the total support given during the research. We as well appreciate all the unalloyed technical and nontechnical supports given by Mrs. Aishat Ayuba and Mrs. Asiya Isa Muhd.

REFERENCES

- [1] S. Hong-Gyoo, Y. Kong-Hyun, Y.Kiyun, J. Soo, Hough Transform for Interior Orientation in Digital Photogrammetry. International Archives of Photogrammetry and Remote Sensing, 2000, 33.
- [2] N. Vassilas, S. Perantonis , E. Charou , T. Tsenoglou, M. Stefouli, S. Varoufakis, Delineation of Lineaments from Satellite Data Based on Efficient Neural Network and Pattern Recognition Techniques. Second Hellenic Conf. an AI SETN2002, Greece, Proceeding Companion, 2002:355~ 366.
- [3] V. Torre, T. Poggio, A.I Memo, On Edge Detection. Report by MIT Artificial Intelligence Laboratory, 1984.
- [4] M. Sharifi, M. Fathy, M. T. Mahmoudi, A Classified and Comparative Study of Edge Detection Algorithms. Proceedings of the International Conference on Information Technology: Coding and Computing, ITCC02, 2002.
- [5] D. Koc San, M. Turker B, Building Extraction From High Resolution Satellite Images Using Hough Transform, International Archives of the Photogrammetry, Remote Sensing and Spatial Information Science, Volume XXXVIII, Part 8, Kyoto Japan , 2010

Big Data and Management of Governmental Services

Omar Saeed Al Mushayt
Department of Administrative and Finance Sciences
King Khalid University, Abha, KSA

Abstract

The term Big Data is different from traditional data in the sense of its nature, variety and velocity. Managing e-government services has become more challenging with the launching of big data.

In this paper, we propose the effectiveness of deploying the techniques and tools of big data in the process of managing governmental services. We show that approach can help to get more quality and governance of governmental services.

1. Introduction:

Big data is considered as a big challenge and critical issue which focus the gorse of e-government in the age of advanced information technology with its applications. Recently American federation authority announced that the amount of global information has been increased sharply and it exceeded the amount of 3 Exabytes (Exabyte is one million petabytes, and betabyte is one million gigabytes) [1] Moreover, the term of big data is different from traditional data in the sense of velocity, variety, and nature. For instant, the high speed of velocity of data comes from E-government is clearly noticeable, where the portals of governments always accept data from state citizens.

US government recognized the importance of big data and was the first who started promoting research in the area of big data and its technical tools for developing complete science and engineering of big data. Big data provides more services to e-government but with new intuitional and technical challenges.

There is a lack of research concentrated and big data and its role in enhancing the services in the sectors of business and e-government [Big data a for digital]. Therefore, we investigate in this paper the affect of applying big data in e-government where we define the governmental services generally, then we explain how can these services be managed and go through e-government services , then we define the term of big data and how can be utilized in e-governmental services and business.

Our paper consists of 3 paragraphs and references. The second one is about the management of E-government services and the third is big data and services managements. Conclusion is in the fourth and last paragraph.

2. Management of Governmental Services:

Management of E-governmental services needs governance tools that work on increasing the quality of data, effectiveness, efficiency and transparency. This management mostly faces many challenges in infrastructure and human factors which are belong to supply and demand sides. So that succeed e-governments meet these challenges with the rate more than 60% [2].

Department	Website	Sources of big data		
		Employees (2010) ⁴	Monthly site visitors* (Quantcast.com)	Sites linking In* (Alexa.com)
1. Agriculture	usda.gov	98,235	2,800,000	69,658
2. Commerce	commerce.gov	45,348	7,700	42,281
3. Defense	defense.gov	771,614	441,100	10,237
4. Education	ed.gov	4,611	2,900,000	53,467
5. Energy	energy.gov	16,651	501,400	24,334
6. Health and Human Services	hhs.gov	83,745	173,200	35,950
7. Housing and Urban Development	hud.gov	9,818	789,700	32,376
8. Homeland Security	dhs.gov	191,197	680,600	21,280
9. Interior	doi.gov	72,168	41,100	6,550
10. Justice	justice.gov	118,104	446,000	19,488
11. Labor	dol.gov	16,554	547,400	23,760
12. State	state.gov	12,086	1,800,000	61,586
13. Transportation	dot.gov	58,189	841,300	36,432
14. Treasury	treasury.gov	112,541	308,100	8,053
15. Veteran Affairs	va.gov	312,878	2,700,000	33,798

Fig. 1. Federal government executives departments with some sources of big data

Generally, a success of any e-government can be measured by the size of the gap between the reality of applied e-government and the designed object and goals of the e-government. Unfortunately, mostly political position plays critical role in the success or fail of the project. Knowledgeable, democratic and strong leaders can work on sustaining success of e-government by their right management. In figure 1, we provide some the executive departments of USA Federal government with their sources of big data.

3. Big Data & Services Management:

In fact, big data is a big institutional and technical challenges face e- government in the era of IT. In literature there are so many research papers deal with big data and business so that to maximize the return on investment, but there is lack of research papers that focus of the public sector of e-government with big data. Public administration should invest the knowledge and techniques of big data. Doing so needs to address the opportunities, challenges, strategies and solutions [3].

Public Sector of services can be managed be utilization of IT by using its tools and techniques but when the number of services is so huge and the data is so big , we need the term of big data to underpin this progress. By changing the policy and legislative laws we can overcame the obstacles of using big data which will enhance the quality of services with lower cost for private and public sectors.

It is wise here to mention the important term Internet of things (IoT) which we define it as network of smart devices that encompass multi-sensors and actuators to measure and act with its environment. IoT has been applied in many areas, such as smart building, homes, healthcare, community, transport (See Fig. 2):

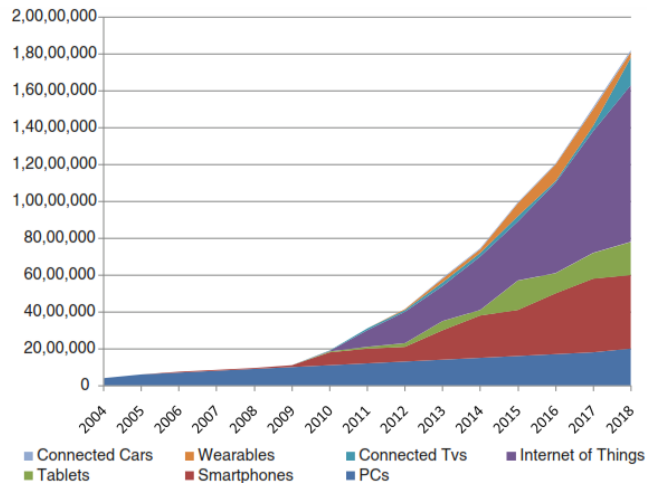


Fig 2. IoT Adapted from Danova (2014)

So big data work on delivering e-government services more effectively and more efficiently. In Figure 3, we provide a model for supporting big data to enhancing the e-governmental services:



Figure 3 A supporting big data model

4. Conclusion

In this paper, we proposed the importance of implanting the techniques and tools of big data in managing the e-government services. We showed that e-Government can reduce the operational costs and improve the quality of services by utilizing the big data with its analytics and increase the outcomes within the right capturing of data and its managements.

References

1. Yu-Che Chen, Tsui-Chuan Hsieh, "big data of digital government : opportunities , challenges", International Journal of Public Administration in the Digital Age, 1(1), 1-14, January-March 2014.
2. Gather a majority of e-government initiations fail on fall short of expectations , gather , inc,s execute programs , San Diego , April 2002.

3. Joseph, R.C.; Johnson, N.A., Big Data and Transformational Government IT Professional, Year: 2013, Volume: 15, Issue: 6
4. V. Morabito, "Data and Analytics for Government Innovation", Springer International Publishing Switzerland 2015.
5. Rajagopalan M.R, Solaimurugan vellaipandiyan , Big Data Framework for National e-Governance Plan, 2013 Eleventh International Conference on ICT and Knowledge Engineering.
6. Feng Ye, Zhijian Wang , Feng Ye, Zhijian Wang, "Cloud-based Big Data Mining & Analyzing Services Platform integrating R", 2013 International Conference on Advanced Cloud and Big Data.
7. IBM. What is big data: Bring big data to the enterprise, 2012, <http://www-01.ibm.com/software/data/bigdata/>
8. F. Zulkernine, M. Bauer, A. Aboulnaga. Towards Cloud-based Analytics-as-a-Service (CLAAaaS) for Big Data Analytics in the Cloud. Santa Clara, 2013 IEEE International Congress on Big Data, 2013, pp. 62-69.

Presenting a Traffic Management and Control System in Driver Assistance Form Based on Vehicular Networks

Arefe Esalat Nejad^{1*} and Morteza Romoozi²

¹Young Researchers and Elite Club, Baft Branch, Islamic Azad University, Baft, Iran.

²Department of Computer Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran.

*Corresponding Author

Abstract

Vehicular Networks is considered a major step in the field of Intelligent Transportation System (ITS). In this technology, some equipment will be installed on vehicles and special places at roadsides which will enable the wireless communication between vehicles with each other and will provide the communication between the vehicles and roadside equipment. One of the ITS application is Traffic monitoring system. Such system enables accessing traffic videos by traffic monitoring centers to make traffic decision. However, providing traffic video for the vehicles can be appealing. This paper addresses a new application in vehicular networks and ITS which can provide this videos for drivers in a city. Each driver request timely traffic video of a location from a web server and the web server forward this request to a stream management server. This server based on current location of the requester vehicle, its speed and its direction calculates appropriate video chunks for each RSU along vehicle destination. This study aims to present a system which can bring a high accessibility for content and can provide it with an appropriate bandwidth and quality for vehicles. Due to the scalability and bandwidth limitations for its content and streaming, vehicular networks are used in this system.

Keywords: Vehicular Networks, ITS, Roadside unit, Traffic monitoring, stream management.

1. Introduction

1.1. ITS Description

Intelligent transportation systems have become common in recent years, especially in optimizing traffic flows. One can mention the applications of this technology in advanced technologies such as intelligent calculations, network communications, visual analysis based on electronic sensors [4,7,10,18-19]. Usually the stability derivation method is applied to traffic models which describe the dynamics of traffic flow [2,14].

Existing ITS solutions detect vehicles in predefined positions. They are based on bulky and power-hungry devices, which use wired technologies for communication and power supply. This increases their installation, maintenance, and reparation cost and subverts the scalability of ITS affecting thus their major objectives [3, 9, 17]. The ITSs attempt to manage optimally the urban traffic by enhancing safety, reducing travel time and fuel consumption at the aim of improving our daily life. It works as a control loop system where it senses traffic and road conditions using surveillance or detection system. The gathered information is communicated to the decision system to be organized and analyzed in order to take appropriate decisions. Figure 1 illustrates a simplified scheme of ITS.

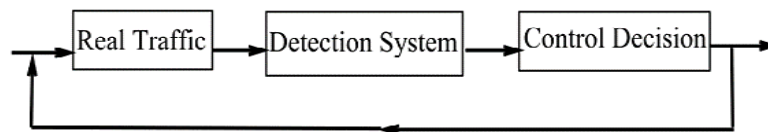


Fig1. ITS mechanism

1.2. Video streaming description

Traffic management and control systems are systems in which various types of receiving and processing information and also transportation traffic management and control are taking place by using automatic tools and related programming. In these systems, vehicles and roadside units are in connection with servers; these servers receive traffic data from the cameras all around the cities and send them to the units.

Video Streaming application for traffic management: video control based on Closed Circuit TV (CCTV) is an important part of traffic control systems [5, 8]. The collected data are sent to Traffic Management Center (TMC). CCTV has problems such as changeability, network cabling costs, and difficulty in giving information to users through internet. Using web cams, TCP/IP networks, and digital network cabling are among solutions for overcoming these problems [1, 12].

In this survey, the video stream rate control is studied considering a normal wireless scenario in which the channel resources are shared among variable number of stations by using a contest-based accessibility control mechanism. In this model, transmittable packages are coded and buffers are allocated to them, and the probability of buffer starvation is investigated. Now, if a package is disrupted, its code will be eliminated and we will enter sending information cycle once again [7, 12, 16].

Some papers investigate the large volume of pictures and difficulty in sending them. Considering the low complexity algorithms and based on background subtraction and error resilience techniques, we try to reduce the transmission bandwidth and obtain a higher frame rate. The results of these researches led to the development of next generation smart cameras suitable for 6LOWPAN. In some methods, innovative video compression is used in video applications. Video compression node with low complexity is based on computer visual techniques and transmission bandwidth reduction by omitting intra-frame external redundancy [6, 11, 15].

1.3. Traffic Monitoring and Modeling

Successful participation in traffic monitoring applications utilizing participatory sensing depends on two factors: the information utility of the estimated traffic condition, and the amount of private information (position and speed) each participant reveals to the server. We believe that vehicular systems based urban traffic monitoring systems will help relieve traffic conditions in the future and help the vehicles to access the information which need it. Traffic monitoring and control is critically important in the highway construction, because traffic monitoring affects the durability and long-term performance of roads. Ensuring subgrade to be compacted as specified is an essential task in traffic monitoring. In this section, we present an architecture based on which will investigate how the chunk demand is sent by vehicles and received from server by RSUs.

1.4. Traffic monitoring challenges

Existence of restrictions on data volume and geographical constraints, as well as the availability of information is a big challenge in traffic monitoring.

1.5. Prediction solution

Therefore we obtained high availability of content in this study that can access it with adequate bandwidth and quality for vehicles. Therefore, in this system assumes the existence of a connection with limited bandwidth. But the limitations of scalability and bandwidth for receipt of content and streaming, we use the vehicular networks. Here you should concentrate on finding the best unit on the roadside as a streaming server for transferring content.

2. Architecture of proposed system

In this section, we present an architecture based on which we will investigate how the chunk demand is sent by vehicles and received from server by RSUs. As you can see in the schematic architecture in figure 2, the cameras which are located all over the location will give their information to video servers; this information will be sent to storage server and its complete specifications such as the exact address where the film is taken, the time when the film is taken, date and size of the film and so on will be stored in video register file. Besides, this information will be given to web server so that it will send the information to network whenever needed. The vehicles in traffic announce the specifications of requested video to

the web server. They send their movement and location information in addition to request specifications. Web server will find the appropriate file for demanding vehicle by connecting to video file register and sends its idea along with location and movement specifications of the demanding vehicle to the stream management server. This server finds the best RSU for transferring the file to vehicle. Or it makes this vehicle a member of multicast structure related to this file.

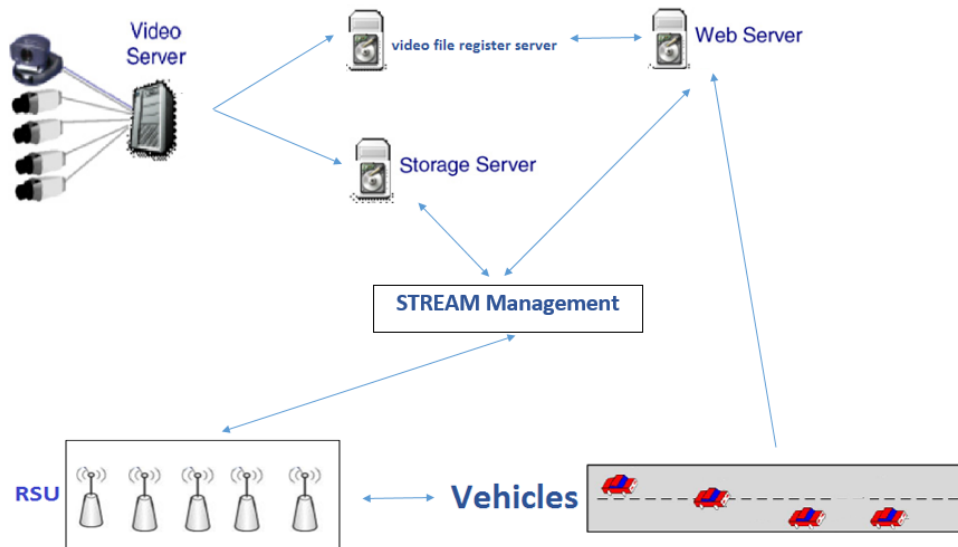


Fig. 2: Suggested architecture for traffic management and control system

2.1. Defined Architecture Components

In this architecture, we simulation a highway with some characterizations: Road side units placed along the highway and in center. Vehicles enter in the roads both sides. RSUs embedded in such way which covered both sides of road. Each RSU have a within range that no one of them have not any interference among each other (Fig3).

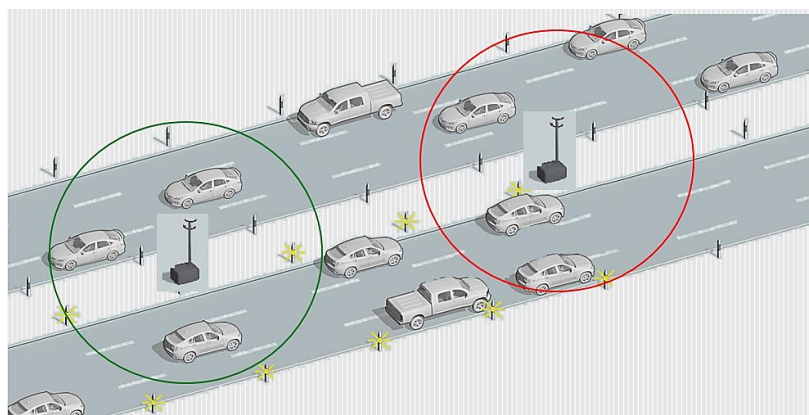


Fig 3. Pattern of embed of RSUs.

The vehicles which enter in the RSU range, they are covered with previous RSU until arrive to next RSU. Each vehicle identify the other vehicle which close to them and with the range

of probability send the advertise message to close vehicle. Then, each vehicle which have any request, send their request message to covered RSU. If vehicle which sent request existence to RSU range, receive request personally but if exit from RSU range, receive request from behind vehicle. This section showed in Fig 4.

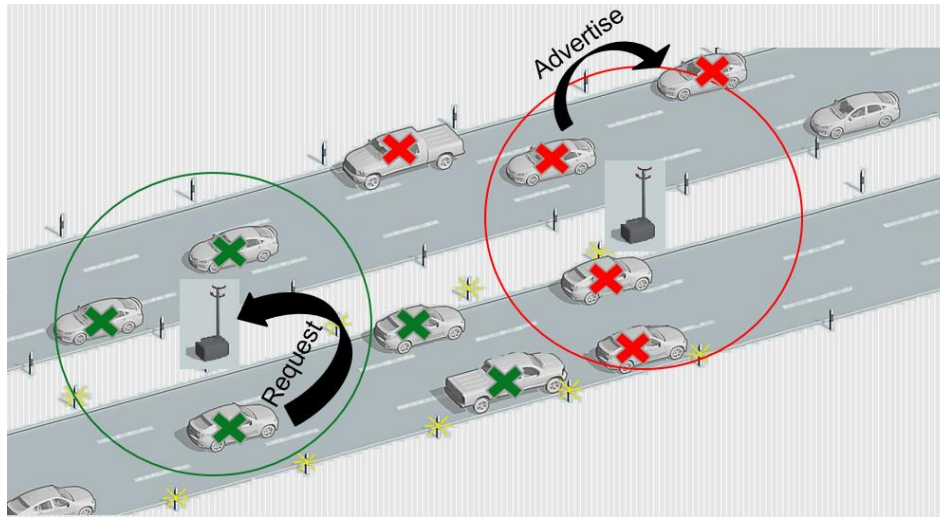


Fig 4. Whole schematic of system performance.

2.2. Stream Management

In this section, stream management has all the file information in a categorized form so that whenever RSU needs them, it will provide the needed information. Each RSU receives a chunk of stream management according to its position which includes the number of vehicles inside its perimeter, the number of vehicles in next RSU, RSU transmission range, and the number of requests which RSU receives. Now, when the vehicle sends its request to RSU, it will receive the information if it is available at range. In this project, our goal is that the vehicle receives the file thoroughly as far as it is covered, i.e., from the time it enters the RSU until it reaches the next RSU. If the vehicle exits its covered radius, it will seek help from the nearest vehicle behind itself which is placed in neighborhood list, both for sending the request and receiving the response. When it reaches the new RSU, It will be covered by the new one and this process happens again. Stream management is the very central server which investigates all the conditions and manages sending and requesting.

2.3. Video Server

Video server is considered a data source which stores all the raw information received from cameras and data centers and sends it to architecture subdivisions. This information is stored in this section without any programming and grouping. This information is sent to storage server and its complete specifications such as exact address of the place of filming, the time of filming, date and size of the film, and so on are stored in video file register. Besides, this information is transferred to web server too, so it will make this information available for network in case of need. The vehicles in traffic announce the requested video specifications

to the web server. They send their movement and location information in addition to the request specifications. By connecting to video file register, the web server finds the appropriate file for the demanding vehicle and sends its ID along with location and movement specifications to the stream management server. This server finds the best RSU for transferring the file to the vehicle. Or it makes this vehicle a member of multicast structure related to this file.

3. Simulation and assessment of results

For assessment of simulation results, we used two fuzzy inference system (mamdani and sugeno) for identify optimize result. The well-known Mamdani fuzzy inference system (MFIS) was first proposed to control a steam engine by a set of linguistic rules obtained from experienced human operators or experts. Since the MFIS uses fuzzy membership functions (MFs) for both input and output variables, it provides intuitive interpretation for human users (Fig 5).

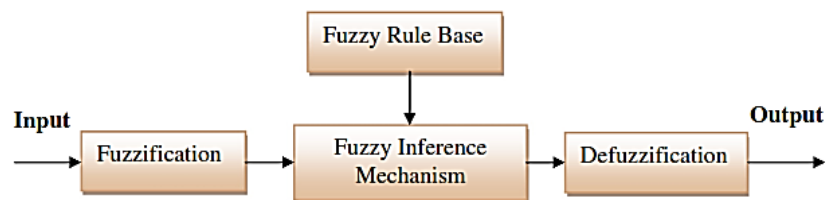


Fig 5. A fuzzy inference system.

3.1. Mamdani system modeling

For determining the destination of each chunk according to the received requests, two systems are investigated:

Mamdani System: This system consists of 4 inputs and one output. The inputs include the distance between vehicle and RSU, the distance between vehicle and next RSU, RSU transmission range, estimating the number of next RSU vehicles (Fig 6).

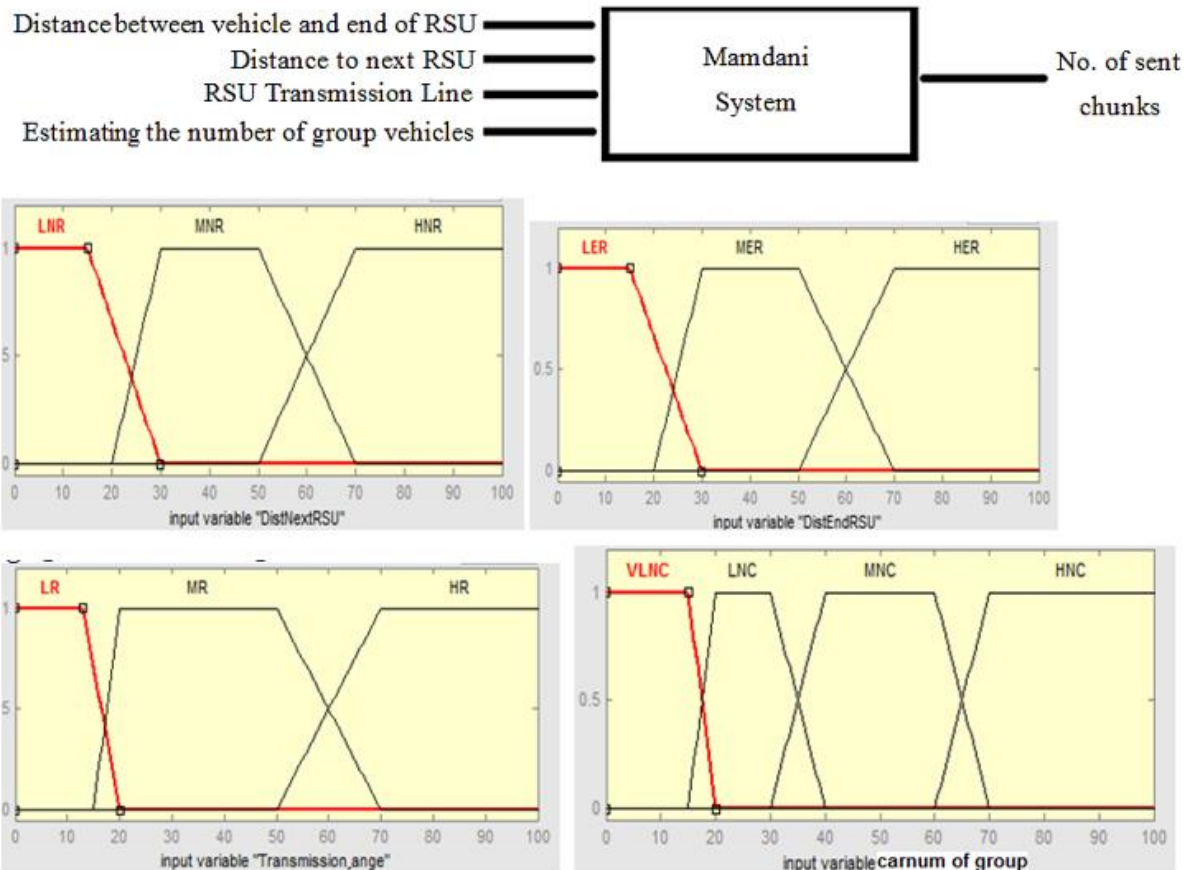


Fig.6. Inputs and outputs of Mamdani system

Each input is specified with low, medium, high, and other fuzzy variables. For estimating the number of group vehicles, we assume that we have k vehicles which are present in the current group. By using Poisson probability distribution function, we obtain the probability that each one stops before reaching the next RSU:

$$\mathbf{K} \times (\text{probability that all continue to move}) = \text{Estimating the number of group vehicles}$$

$$\text{The probability that all continue to move} = \prod_0^{\text{carnum}} (1 - P_{si})$$

This system, which was designed, will be called as a function in the application, and it gives us the output after receiving inputs from the application.

3.2. Sugeno system modeling

We have two kinds of file receiving in this system: one which is done directly (when the vehicle is in the range of RSU), and one in assistance form or vehicle-to-vehicle (when the demanding vehicle exits the RSU range).

$$C_{in} = \left(\frac{d_{rem}}{V} \times r_{RSU} \right) / N_T$$

$$C_{Tco1} = \frac{d_{RSU-RSV}}{V} \times r_{Co}$$

$$C_{Tco2} = \left(\left(\frac{N \times d_{ist}}{V} \right) \times r_{RSD} \right) / N_T$$

$$Z = A \times C_{in} + B \times (\min(C_{Tco1}, C_{Tco2})) \quad (0 < A, B \leq 1)$$

C_{in} = the receivable volume of the system in direct way, C_{tco2} = the remainder distance for the group, Z = the receivable capacity by group vehicles, C_{tco1} = the receivable volume in assistance form.

3.3. System Functional Modes

The simulation of the system is done in a way that all the considered modes can be executed. We list a number of system functional modes in this section. We keep the width and lengths of the highway fixed and increase the number of input vehicles. We increase the length and the number of RSUs and change the number of vehicles, and many modes can be executed in this way.

3.3.1. Scenario 1

In this section of simulation, we have provided the most ideal conditions of the application: a highway with a length of 200 m and RSU number of 5. In this mode, 8 vehicles are covered by RSU and send their request to RSU unit under the best conditions and receive their responses (Fig 7).

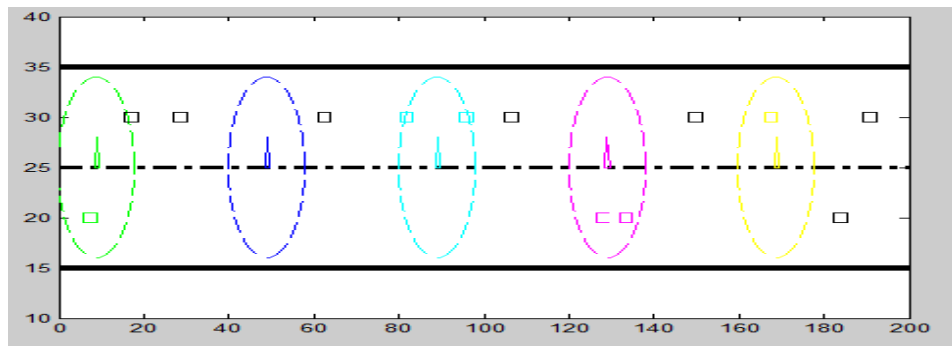


Fig. 7. Performing simulation for 8 vehicles which are covered

3.3.2. Scenario 2

In this section of simulation, we have increased the number of input vehicles in a highway with a length of 200 m and 5 RSUs. In this mode, 15 vehicles are covered by RSUs and send their request to RSU unit and receive their responses after conducted investigations. In this functional mode, the simulation time increases because all the inputs and outputs should be investigated both in Mamdani and sugeno systems (Fig 8).

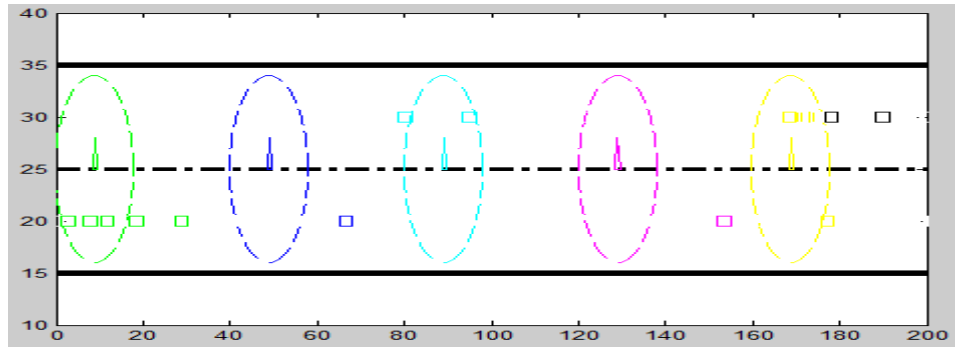


Fig.8. Performing simulation for 15 vehicles

3.3.3. Scenario 3

In this section of simulation, we increase the highway length to 350 m and consider the number of RSUs equal to 8. In the initial application, the conditions are in such a way that if we increase or decrease the length of highway and do not change the RSU number, error will occur in running the application. In this mode, 8 vehicles will be covered by RSUs and send their requests to RSU unit and receive the responses after conducted investigations. In this section, the vehicles can send more requests, because the number of RSUs has increased and vehicles can send more requests to them(Fig 9).

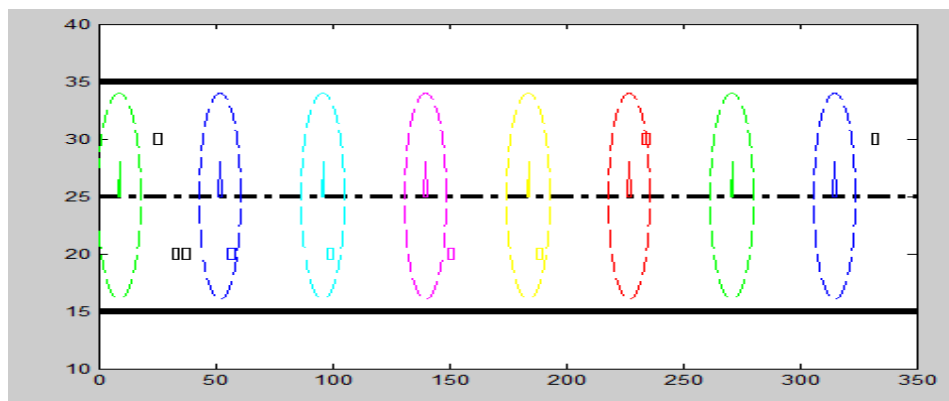


Fig. 9. Simulation for 8 RSUs and a highway with a length of 350 m

3.3.4. Scenario 4

In this section of simulation, we have a highway with a length of 200 m and a number of 5 RSUs. In this mode, we changed the number of vehicles from 5-12 to 5-25. In this mode, the number of vehicles covered by RSU increases and more requests are received by RSU, and they receive their responses after the conducted investigations(Fig 10).

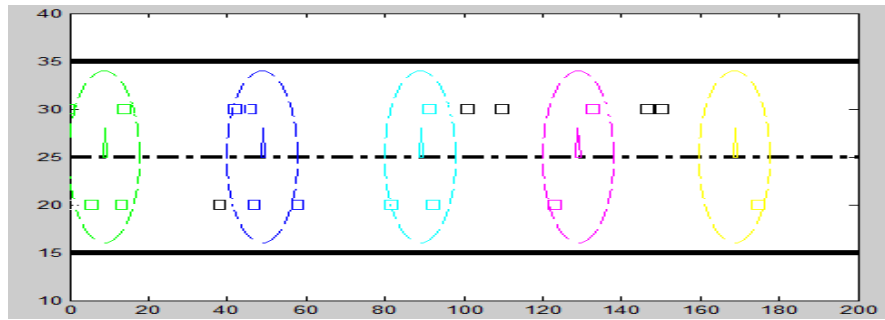


Fig. 10. Changing the range of random vehicles from 5-15 to 5-25

3.3.5. Scenario 5

In this section of simulation, we have increased the highway length to 350 m and considered the RSU number equal to 8. In this mode, we changed the number of vehicles from 5-15 to 5-25. In this mode, the number of vehicles which are covered increases and more requests are received by RSU, and the vehicles receive their responses after the conducted investigations (Fig 11).

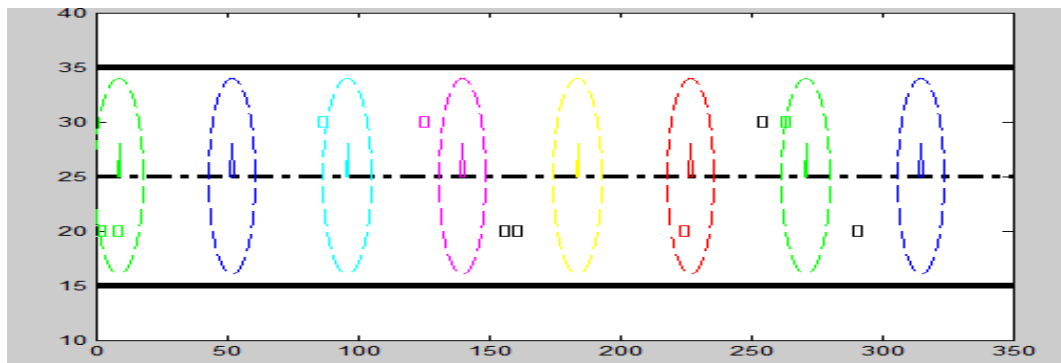


Fig. 11. Changing the range of random vehicles from 5-15 to 5-25 and changing the number of RSUs and the length of highway

3.4. Parameters

Parameters which used in this simulation include: Long of highway, Number of RSU, Location of RSU, Counter of vehicle, Location of vehicle, vehicle speed, vehicle direction, Distance to end RSU, Distance to next RSU, Transmission range of RSU, RSU bandwidth, Transmission Bandwidth as contributor, Distance between vehicles and number of vehicles in RSU that all of them are variable except Location of RSU and Distance between vehicles.

3.5. Metrics

We present two metrics for this study:

3.5.1. Metric 1: Rate of successful receive for RSU

$$\text{Rate of successful Receive} = \frac{\text{Number of successful Receive}}{\text{Total Requests}} \times \begin{matrix} \text{OUT 1} \Rightarrow \text{Mamdani Output} \\ \text{or} \\ \text{OUT 2} \Rightarrow \text{Sugeno Output} \end{matrix}$$

3.5.2. Metric 2: Receive time per Chunk for RSU

$$\text{Receive Time per Chunk} = \frac{T_{total}}{N} \times \begin{matrix} \text{OUT 1} \Rightarrow \text{Mamdani Output} \\ \text{or} \\ \text{OUT 2} \Rightarrow \text{Sugeno Output} \end{matrix}$$

$$(T_{total} = \text{Total Time} \ \& \ N = \text{Number of Received Chunk})$$

Scenarios

Tables 1-3 showed Mamdani system inputs and outputs for vehicles per variable M and RSUTR.

Table 1: Mamdani system inputs and outputs for 9 vehicles per M = 11 and RSUTR = 66

Inputs			Output	
Distance to end of RSU	RSU Transmission range(RSUTR)	Number of group vehicle(M)	Distance to next RSU	Number of sent chunks
9,02.7	77	11	34,004.	1.8,0490
0,0.47	77	11	30,038.	1.8,0490
6,0.11	77	11	14,0209	101,8777
10,0764	77	11	30,1.98	1.8,0490
10,0.829	77	11	9,3879	101,8777
11,8393	77	11	.	101,8777
11,8393	77	11	37,8727	1.8,0490
.	77	11	17,720.	101,8777
13,7774	77	11	38,81.8	1.8,0490

Table 2: Mamdani system inputs and outputs for 9 vehicles per M = 10 and RSUTR = 55

Inputs			Output	
Distance to end of RSU	RSU Transmission range(RSUTR)	Number of group vehicle(M)	Distance to next RSU	Number of sent chunks
6.7713	55	10	31,8047	82,4828
3,3621	55	10	28,3955	77,2643
4.2344	55	10	12,9710	52,1965
8,2011	55	10	33,2345	82,4828
.	55	10	7,9867	52,1965
9,0752	55	10	.	52,1965
8,9880	55	10	34,0214	82,4828
9.1212	55	10	15,1195	52,1965
11,0715	55	10	36,1040	82,4828

Table 3: Sugeno system inputs and outputs for 9 vehicles.

Inputs			Output
the receivable volume of the system in direct way	the receivable volume in assistance form	Residual distance for group	Number of sent chunks
171,1418	145,4871	0,1819	52,0516
101,5623	243,5217	0,2029	30,5904
123,3453	379,1908	0,1878	37,1132
268,6562	213,2951	0,2666	80,7568
170,5653	285,4699	0,1898	51,2828
151,9613	156,8593	0,1307	45,6668
207,6172	140,2906	0,1754	62,3904
301,4353	249,1518	0,2021	90,5532
509,1635	147,8255	0,3696	152,9708

The blue diagram represents Mamdani system and the red diagram represents sugeno system. We consider the number of vehicles in the range of 5 to 50. We have limited the RSUs in simulation system so that they can respond to three requests simultaneously. The results are collected in a way that different times of simulation have been performed and

the gathered data have been averaged. As it can be seen in the diagram, the Mamdani system has more cohesion and less fluctuation compared to sugeno system and hence it is a better respondent. As the number of the vehicles increases, the amount of received file decreases, because RSU is responsible to answer limited requests and requests which have arrived earlier.

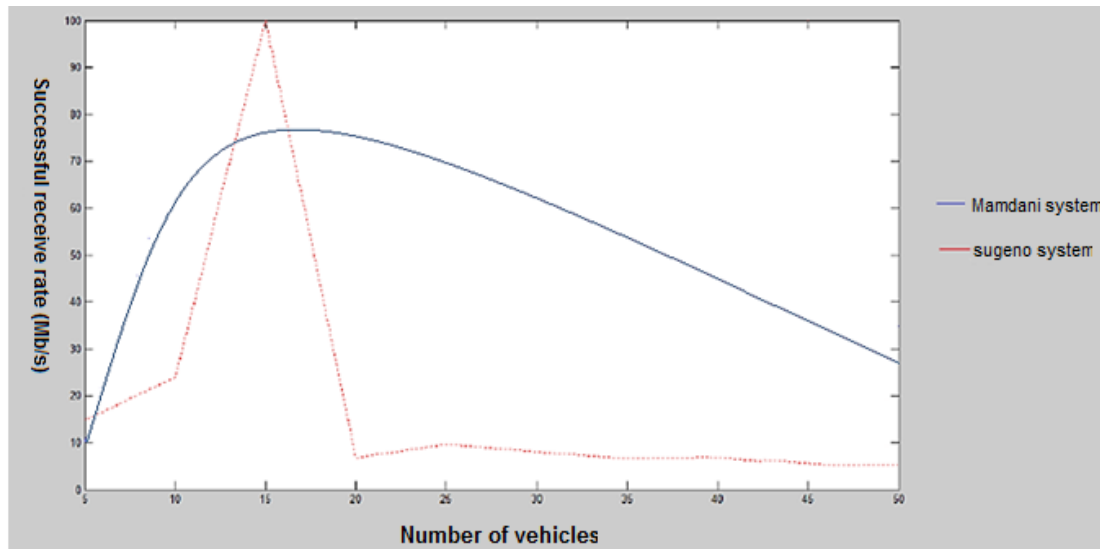


Fig. 8: The output diagram of successful receive rate of sugeno and Mamdani systems based on the number of vehicles

In the following diagram, the receiving time for each chunk is investigated based on the number of vehicles. The diagram proceeds in the same way, but as the number of vehicles increase, the receiving time decreases in sugeno system compared to Mamdani system.

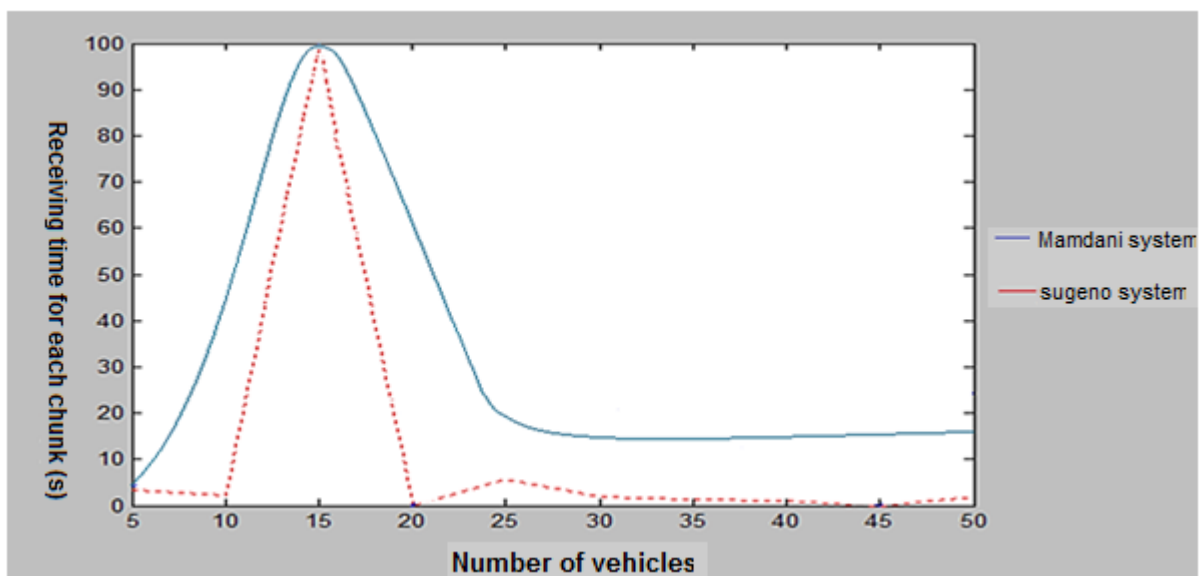


Fig. 9: The output diagram of receiving time for each chunk in Mamdani and sugeno systems based on the number of vehicles

Another mode in which we investigate the diagrams is based on the RSU number. In fundamental simulation system, the number we considered for RSU is equal to 5, so as this number increases, the performance of the system decreases. This change is similar for both systems, although we have better efficiency in sugeno system with less RSU number.

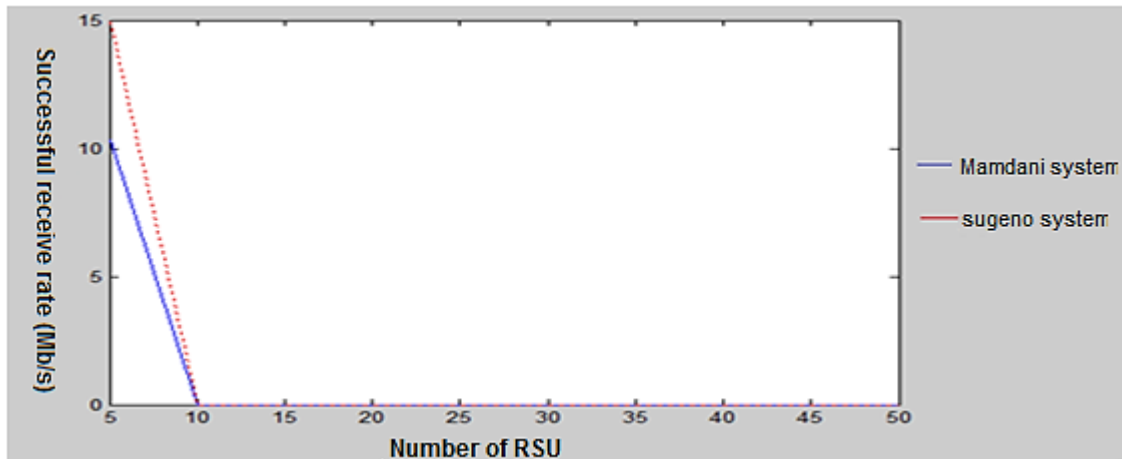


Fig. 10: The output diagram of successful receive rate for sugeno and Mamdani systems based on the number of RSUs

In receiving time for each chunk in sugeno system, it takes less time to receive files, but Mamdani system has a lot of fluctuation and this fluctuation does not match with file receiving.

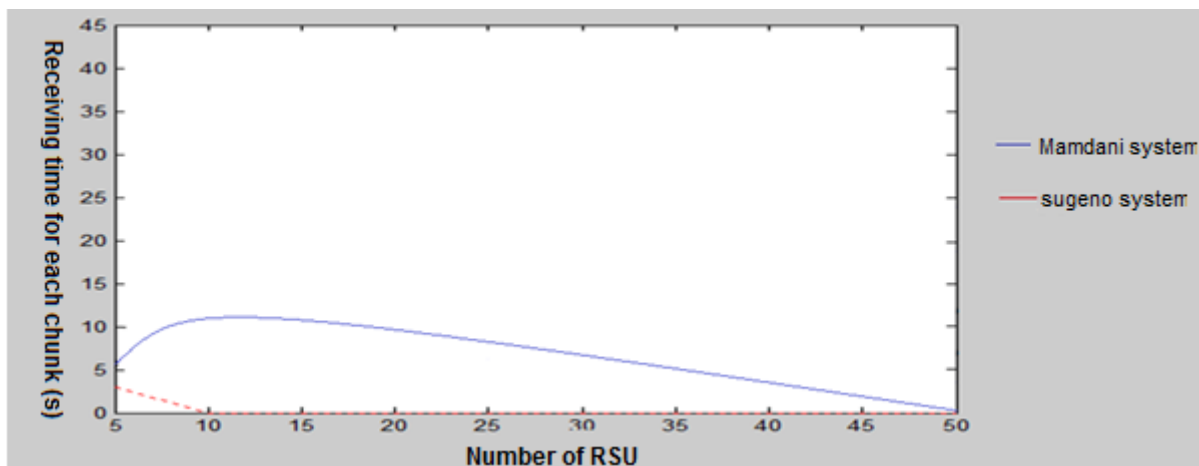


Fig. 11: The output diagram of receiving time for each chunk in Mamdani and sugeno systems based on the number of RSUs

In this section of the research, the fuzzy Mamdani and sugeno diagrams will be investigated based on the vehicles speed. In this section, changes in Mamdani are less

than sugeno changes. But in sugeno, more files are received until the speed of 20, but this receiving rate immediately reaches zero at some speeds.

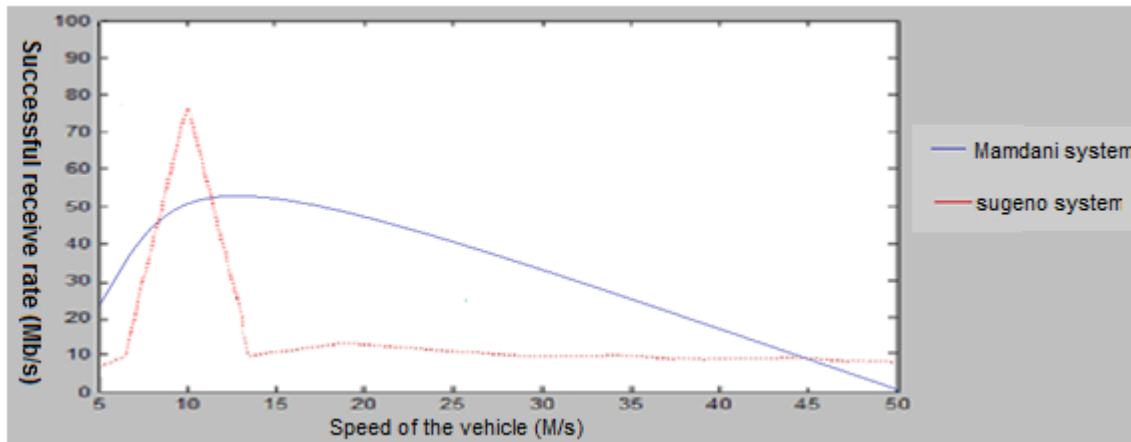


Fig. 12: The output diagram of successful receive rate for sugeno and Mamdani systems based on speed of the vehicle

In explaining the following diagram, we can say that receiving time intervals in Mamdani systems are more logical than sugeno system. According to the given formula, it is revealed in this section that based on the number of the chunks and system output, Mamdani system has a better response.

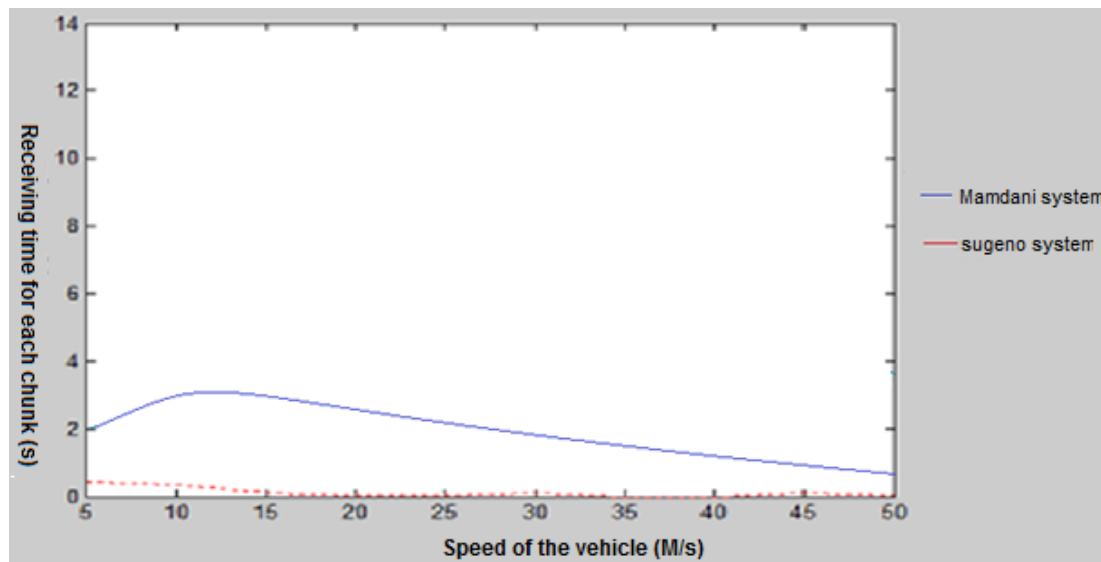


Fig. 13: The output diagram of receiving time for each chunk in Mamdani and sugeno systems based on speed of the vehicle

Conclusion

Nowadays, traffic management and control systems cover a large portion of traffic projects. Due to the vehicles traffic on the roads, the security and health of travelers is of

great importance. In the section of urban traffic, making the traffic system intelligent will be a great contribution to vehicles control. Using cameras all over the city, especially at intersections and crossroads, can decrease the volume of traffic and prevent car accidents. The vehicles are equipped with intelligent sensors in such systems in order to receive the environmental information. The roadside units are responsible for transferring the information from central system to vehicles. Roads and highways are going through the intelligent making evolution by locating roadside units and connecting them to central server and receiving information from cameras. If a vehicle is moving on a highway and needs information, it can receive that information from roadside units. Information such as the upcoming weather conditions, incidents such as occurred accidents, recreational-touristic places along the road, getting music or desired videos can be achieved from these roadside units. In the designed system, we will determine the number of RSUs based according to the length of highway in order to cover the entire road. The number of vehicles which enter the highway will do the sending and receiving of the desired files. In this study, we have omitted the geographical and bandwidth limitations as much as possible. If the RSU transmission range is high and it is located regularly and without interference at certain locations of the road, every vehicle that enters the road will send the request to RSU in case of need and will receive the requested file based on its location (distance to the end of RSU, distance to the next RSU, the number of vehicles in next RSU, RSU transmission range). The amount of files, which each RSU receives from stream management, depends on the requests and vehicles, which enter the RSU. We can use multicast algorithms in future works to create better conditions.

References

1. Agui, K.G, Fehon, K.J, Raie, R., Designing a traffic management system to utilize a digital cable network. In: Proceedings of the IEEE international conference on intelligent transportation systems, Oakland, CA, USA, 2001, p. 1044–9.
2. Brackstone, M., McDonald, M., Car-following: A historical review car-following: a historical review. Transp Res Part F, 2000, 2, 181–96.
3. Brett, T., Trivedi, M., A novel interactivity environment for integrated intelligent transportation and telematic systems. In: Proceedings of the IEEE international conference on intelligent transportation systems, 2002, p: 340–5.
4. Cheng, F.C, Huang, S.C., Efficient histogram modification using bilateral Bezier curve for the contrast enhancement, J. Display Technol., 2013, 9, 44–50.
5. Gettman, D., O'Keeffe, D., AGUIGUI, K., Tighe, W., Van Dillen, D., Cormier, B., Innovative, ethernet-based communications network architecture for integrated transportation management systems. In: Proceedings ITS World Congress, Chicago, IL, 2002, p: 1000–8.

6. Helbing, D., Hennecke, A., Shvetsov, V., Treiber, M., Traffic flow dynamics traffic flow dynamics. Germany, Springer, 2013.
7. Huang, S.C., Cheng, F.C., Chiu, Y.S., Efficient contrast enhancement using adaptive gamma correction with weighting distribution, IEEE Trans. Image Process, 2013, 22 .1032–1041.
8. Lighthill, M.H., Whitham, G.B., On kinematic waves 2: a theory of traffic flow on long, crowded roads. Proc R Soc London a, 1955, 229, p: 317–45.
9. Peng, G., Nie F., Cao, B., Liu, C., A driver's memory lattice model of traffic flow and its numerical simulation. Nonlinear Dyn, 2012, 67, 18, p: 11–5.
10. Popoola, O., Wang, K.: Video-based abnormal human behavior recognition-a review, IEEE Trans. Syst., Man, Cybernet., Part C: Appl. Rev., 2012, 42, p: 865–878.
11. Salvadori, C., Petracca, M., Pelliccia, R., Ghibaudi, M., Pagano, P., Video streaming in wireless sensor networks with low-complexity change detection enforcement, in: Baltic Congress on Future Internet Communications, 2012, pp. 8–13.
12. Santini, S., Analysis of traffic flow in urban areas using web cameras. In: Proceedings of IEEE workshop on applications of computer vision, Palm Springs, CA, USA, 2000, p: 140–5.
13. Tampere, C.M.J., Hoogendoorn, S.P., van Arem, B., A behavioural approach to instability, stop and go waves, wide jams and capacity drop. In: Proceedings of the 16th international symposium on transportation and traffic theory, 2005, p: 205–28.
14. Tang, T.Q, Wang, Y., Yang, X., Wu, Y., A new car-following model accounting for varying road condition. Nonlinear Dyn, 2012, 70, p: 397–405.
15. Tian, C., Sun, D., Zhang, M., Effect of the optimal velocity function on traffic phase transitions in lattice hydrodynamic models. Commun Nonlinear Sci Numer Simul, 2011, 16:452, p: 4–9.
16. Tickoo, O., Sikdar, B., On the impact of IEEE 802.11 MAC on traffic characteristics, IEEE Journal on Selected Areas in Communications, 2003, 21.
17. Wilson, R.E, Berg, P., Hooper, S., Lunt, G., Many neighbour interaction and non-locality in traffic models. The Eur Phys J B, 2004, 39, p: 397–408.
18. Xu, Y., Xu, D., Lin, S., Han, T., Cao, X., Li, X., Detection of sudden pedestrian crossings for driving assistance systems, IEEE Trans. Syst., Man, Cybernet., Part B: Cybernet., 2012, 42, p:729–739.
19. Yeh, C.H., Lin, C.Y., Muchtar, K., Kang, L.W., Real-time background modeling based on a multi-level texture description, Inform. Sci., 2014, 269, p:106–127.

Facial Expression Recognition via MapReduce Assisted k-Nearest Neighbor Algorithm

Assis. Lecture. Jaafar Sadiq Qateef, Assis. Lecture Ammar Awad Kazm

Computer Science Department- College of Education-Wasit university-Iraq

Abstract

Accurate recognition and differentiation of the human facial expressions require substantial computational power, where the efficiency of algorithm plays a vital role. Recent advancement in the human computer interaction and object recognition in terms of facial expressions and gesture demanded realistic facial animation models, smart algorithms for massive data handling, as well as sophisticated graphical user interfaces. A rapid escalation in the photo upload to the online social networks web sites such as Facebook and Twitter is evident, where huge dataset handling became the key issue. Competent search and manipulations within a large dataset for image reproductions posed a new challenge, where standard tools cannot achieve the desired target. Often, images possessing intricate multidimensional attributes involve robust computational techniques for pragmatic recognition. Thus, developing a novel robust facial recognition platform emerged as an urgent necessity. We introduce a new algorithm for facial image tagging and classification in cloud environments using the Hadoop and MapReduce based k-nearest neighbor algorithms. Experiments are performed on 3120 images from 120 individuals (65 male, 55 female) from the AR Face Database. The efficiency of the proposed algorithm is evaluated in terms of recognition rates and processing time. Significant improvements in the performance are demonstrated.

Keywords: Facial expression recognition, MapReduce, Hadoop, k-nearest neighbor.

1. INTRODUCTION

Human face being majorly the significant art object and innermost characteristic of phenotype plays a vital role in the interactions with computer. Furthermore, facial appearances being fundamental to human social interaction are often exploited to identify the origin, emotional attributes, health conditions, and psychology. Human face is the visible mirror reflection of important information. Thus, facial recognition is considered as many innate reflexive cognitive competencies. Certainly, achieving an accurate face recognition technique became prospective in network multimedia society [1]. Face recognition became a specialized research domain and contributed tremendously towards the field of computer vision, human aided virtual reality and game environment. Commercial systems are ranged from security to an intelligent view depending on human computer interaction (HCI). These applications include automated crowd observations for recognizing criminals in public spaces [2], the private property access control [3], mug-shot identification [4], facial reconstruction [5], HCI design [6], etc. to cite a few.

The dimensionality reduction of a high dimensional datasets prior to the implementation of k-nearest-neighbors (KNN) algorithm is prerequisite to circumvent the startling effects originate from the so called '*curse of dimensionality*' [7]. This procedure involves principal component analysis (PCA), linear discriminant analysis (LDA), and canonical correlation analysis (CCA) in the phase preprocessing. Finally, the KNN algorithm is implemented to the spatial feature vectors to reducing the dimension. Face recognition is a challenging and sophisticated task due to the involvement of various complicated factors such as the alterations in illumination, facial expression, pose, accessories, and age. On top, the physical and physiological state of human emotion play decisive role in facial appearances (color and texture), which often changes as we move, talk, and suffer stress. Despite much research a correlation among the facial color, pigments homogeneity or skin quality under stimuli even for basic natural emotional expressions is far from being achieved.

The HCI administrator need to determine the surf features of photos for calculating the distances to a common reference point so that a comparison with the reference data can be made. Most of the face recognition techniques that are developed during the 1980s and 1990s are not efficient in handling multidimensional data efficiently. Kirby and Sirovich [8] developed an effective PCA algorithm for facial images and minimized the MSE (mean squared error) between the original images and their reconstructions. This is based on "*eigenvector analysis*". Turk and Pentland [9, 10], and Fleming [11], also used the PCA algorithm for face recognition.

The main idea of using PCA algorithm for face recognition is to represent a large one dimensional vector of pixels that is structured from a 2-D facial image to the compact principal components of feature space called Eigen space projection. The Eigen space is constructed by the set of eigenvectors of covariance matrix that can be imparted from a set of training facial images [12]. Although, known humans faces may be identified, but dealing with huge number of unknown faces to distinguishing them is difficult. However, the computer vision applications using only a few number of input images have the difficulty in gaining computational resources and storage. Similarity, the development of the applications that use a large number of images are limited. It is often suitable to run these algorithms for a large datasets that are actually limited by a computational power of single computer [13]. These limitations associated with face detection and recognition is overcome using parallel processing.

Hadoop being a computationally robust distributed processing platform uses a collection of additional software for processing a number of datasets in parallel. It provides an open source system based on cloud that can process data across multiple machines as well as in multiple environment. Conversely, MapReduce mechanism of parallel computing module embraces the dividing and the conquering approach [14]. We design and implement a Hadoop based face recognition system using PCA and KNN for image classification and tagging in cloud environments.

2. Hadoop Ecosystem

It is important to justify the implementation of Hadoop platform for media processing by highlighting the drawbacks of the existing facial recognition system.

- i. The result on queries is inefficient and limited because the multimedia data within the existing system is retained in a centralized data store. The storage system bandwidth becomes a bottleneck and prevents the overall query performance when dealing with a multiple queries.
- ii. The poor in reliability and accidental errors in the cluster server can cause a research failure because of incompetence to automatic recovery.
- iii. The limited management and maintenance capabilities lacks the system for overall monitoring, extending the hardware and the software infrastructures in real time to make response of operations [15]. However, strong distribution of Hadoop together with the manifold coding efficiencies across the infrastructure with improved performance for energy consumption, capacity requirements for servers and storage controllers offers it as a suitable platform. Using Hadoop, the required time for analyzing different media information can substantially be shortened compared to the traditional platforms. Furthermore, the bandwidth can be maximized and total production can remarkably be improved employing Hadoop as multimedia processing platform.

3. Hadoop Parallel Processing System for Face Recognition

Hadoop is comprised of two components including the Hadoop Distributed File System (HDFS) [16] and MapReduce [17], where the former one is designed for reliable storage across clusters and the later one is a framework for parallel distributed processing. The customary MapReduce program contains a pair of user defined functions called map/reduce functions. The map function takes key value pairs $\{k_1, v_1\}$ as input and results a partitioned sorted set $\{k_2, v_2\}$ as the intermediate output. Conversely, the reduce function takes the $[k_2, \text{list}\{v_2\}]$ pairs, where $\text{list}\{v_2\}$ is the list of whole values that are belong to k_2 . It results another key value pairs (k_3, v_3) as the final output and so on.

The Hadoop is constructed for the batch processing and also termed as the “*divide and conquer*” strategy. This strategy considers a dataset all at once and in plenty as input prior to the data processing to produce a large output. The real time stream processing became feasible with the Yarn’s version [16]. This is beneficial for the organizations and individuals including police, insurance agents, firefighters, etc. Figure 1 displays the basic structure of Hadoop system on the cloud. The Hadoop platform serves two primary design goals: (i) The real-time analysis for processing a collection of images from social platforms by keeping the feature information in cloud storage, and (ii) the real-time observation and retrieval for determining similarities and displaying the feedback to the users.

The main algorithm of the Hadoop system considers the following aspects:

i. Linear Subspace Analysis

Several methods are introduced for face recognition [18], in which most of them depend on a representation of the images to prompt a vector space structure. The image data can be represented as vectors such as points in high dimensional vector space. For instance, a 2-dimensional (2D) image can be mapped to a vector by lexicographic ordering of the pixel elements by concatenating each row or column in the image. Let, $X = (x_1, x_2, \dots, x_n)$ represents N images, where X is the face vector of the dimension, concatenated from each facial image. Here, $n = P \times Q$, where n represents the number of pixels in the facial image. The PCA is the standard linear appearance based classifiers that project the face vector to the feature space. The projected coefficients are used to signify the weights of each facial image in the feature space. The grade of similarity between the test images and the training images is measured between their projected coefficients vectors and the larger the grade of similarity. The projection procedure can be represented as a linear transformation from the original image vector to the projected vector $V_f = WTX$, where T is the feature vector matrix that is extracted from data of the matrix X , W is the transformation matrix with dimension of V_f lower than X .

ii. Principal Component Analysis

The Eigen face algorithm uses component analysis to reducing the original dimension to find the vectors that can be considered as the best choice for the distribution of facial images within the entire image space. The resulting vectors called “face space” define the subspace of face images. This face space can be projected from the training image. Thus, a set of weights that determines the contribution of all vector in the face space is termed as “feature vector.” These feature vectors can also be used to improve the accuracy (used multiple feature vectors). The identified test image must project the test image onto the face space to get the corresponding set of weights, yielding the so called “projected vector.” The face in the test image can be specified by making the comparison between the incoming projected vector and the stored feature vectors.

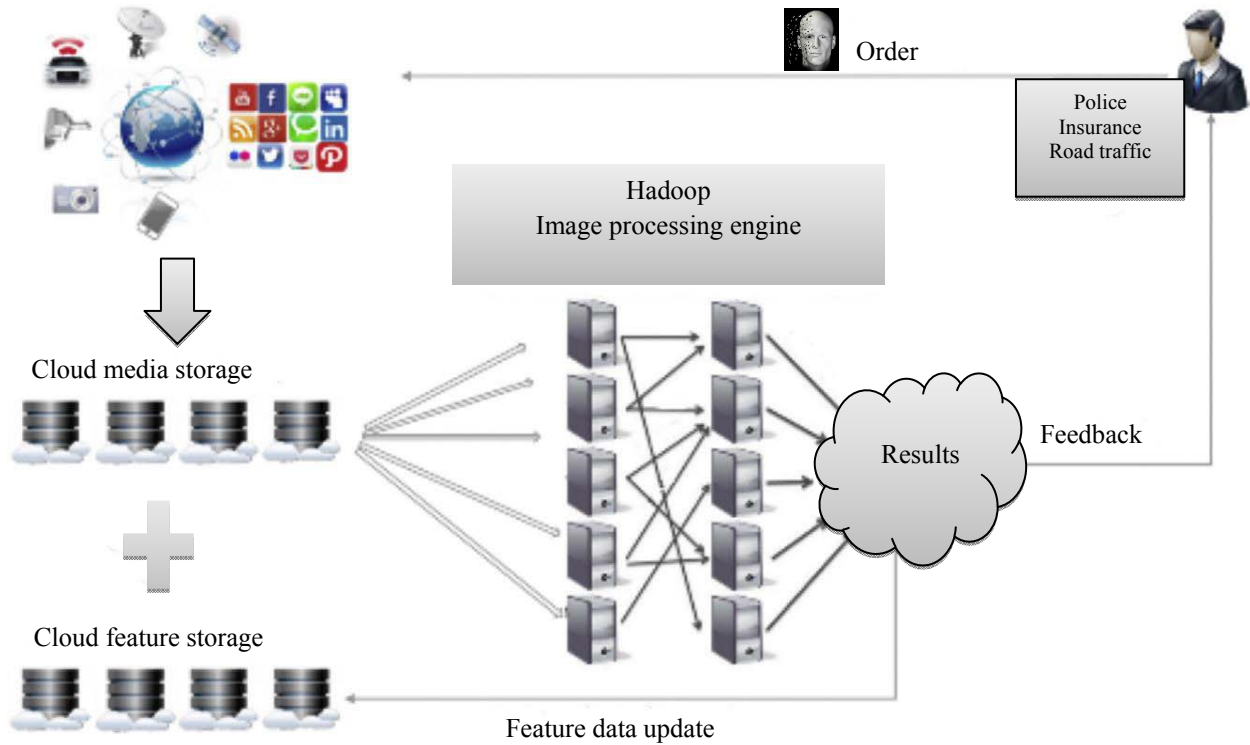


Figure 1: Basic architecture of Hadoop image processing system on the cloud environment.

Let us consider N number of 2D facial image each having R rows and C columns expressed in the form of a matrix:

$$X = \begin{bmatrix} x_{11} & \cdots & x_{N1} \\ \vdots & \ddots & \vdots \\ x_{1n} & \cdots & x_{Nn} \end{bmatrix}$$

The average of images is obtained by subtracting the mean image from each image vector using the expression:

$$\bar{X} = \frac{1}{N} \sum_{i=1}^N x_i \quad (1)$$

The mean centered image (X') is obtained by subtracting the mean image from each input image as follows:

$$X' = [x'_1, x'_2, \dots, x'_i, \dots, x'_N] \text{ and } x'_i = x_i - \bar{X} \quad (2)$$

The set of features with the largest possible projection into X' is determined using 'Eigen-decomposition' procedure. A group of eigenvectors (E) and eigenvalues (λ) of the covariance matrix are obtained via:

$$C = X'X'^T$$

$$\lambda = [\lambda_1, \lambda_2, \dots, \lambda_i, \dots, \lambda_n] \text{ and } E = [e_1, e_2, \dots, e_i, \dots, e_n]$$

The eigenvalue equation takes the form:

$$X'X'^T e_i = \lambda_i e_i \quad (3)$$

Based on the similar eigenvalues, these eigenvectors are usually arranged in descending order. Eigenvector associated with the major Eigenvalue is usually the one that reflects the maximum variance inside image and the rest fall exponentially. Thus, the first 5 to 10% of the proportions achieves 90% of the complete variance. Nonetheless, this size with the matrix G ($n \times n$) is too big to look for all the eigenvectors and eigenvalues, which is computationally unfeasible. Contemplating G as an alternative such that:

$$C' = X'^T X' \\ \lambda' = [\lambda'_1, \lambda'_2, \dots, \lambda'_i, \dots, \lambda'_N] \text{ and } E' = [e'_1, e'_2, \dots, e'_i, \dots, e'_N]$$

are the eigenvalues and eigenvectors of C then one obtains:

$$X'^T X' e'_i = \lambda'_i e'_i$$

Multiplying both sides by X one gets:

$$X'X'^T X' e'_i = X' \lambda' E' = \lambda'_i X' e'_i \quad (4)$$

Eqs. (3) And (4) are compared to get the eigenvectors of $C = X'X'^T$. Thus, ($N \times N$) matrix is assembled to find N eigenvectors, which usually ascertain the linear permutations from the N training collection face images to form the Eigen faces.

In the event, N eigenvectors are chosen using Eq. (3):

$$E_{\text{the first } N \text{ eigenvectors}} = X' E''$$

In practice, the training list of images are reasonably little and the computations is manageable. The eigenvectors age span some sort of schedule established using experience graphics to the eigenrspace. For N training image, N significant eigenvectors are selected because they have the most important linked eigenvalues, $N' \leq N$. For each and every known particular (each list of training images), some sort of facial image may be forecasted upon eigenspace E' ($N \times N'$ dimensions). The feature vector pertaining to N eigenvectors can be built for N (often as little as one) feature vectors from N training images for each and every training set.

The first feature vectors are always opted. $1 \leq \zeta \leq N'$

For P sets of training images one obtains,

$$X = [X_1, X_2, \dots, X_i, \dots, X_p] \\ C = [C_1, C_2, \dots, C_i, \dots, C_p]$$

Here one class is issued for every image set, hence the average representation for every set follows:

$$\bar{X} = [\bar{X}_1, \bar{X}_2, \dots, \bar{X}_i, \dots, \bar{X}_p] \text{ and } 1 \leq i \leq p \quad (5)$$

The feature $\Omega = [\Omega_1, \Omega_2, \dots, \Omega_i, \dots, \Omega_p]$ vectors for classes yields: $\Omega_i = [v_{i1}, v_{i2}, \dots, v_{ij}, \dots, v_{i\zeta}]^T$

Provided a good unfamiliar face image \mathbf{F} , forced to always be focused and also with the similar sizing as the training image, we've got $\hat{\psi}_i = \mathbf{F} - \bar{X}_i$ in which X_i could be the suggest impression. And then we all project ψ_i in the encounter space E_i involving C_i , so that you can obtain the projected vector $\psi = [\psi_1, \psi_2, \dots, \psi_i, \dots, \psi_p]$ via each and every encounter space, in which ψ_i provides a vector involving weight load which represents the side of the bargain of each and every eigenvector encounter to the reconstruction with the granted image for every class:

$$\psi_i = [\omega_{i1}, \omega_{i2}, \dots, \omega_{ij}, \dots, \omega_{i\zeta}]^T, 1 \leq i \leq p, 1 \leq j \leq \zeta, \omega_{ij} = (v_{ij}^T \hat{\psi}_i)$$

Where ω_{ij} is the j th weight in the vector ψ_i . Consequently, the simplest means for deciding the face class is to find the face class C which decreases the particular Euclidean length:

$$\varepsilon_\varphi = \|(\psi_i - v_{ij})\| \text{ and } \varepsilon_\varphi \ll \theta_\varepsilon, 1 \leq i \leq p, 1 \leq j \leq \zeta \quad (6)$$

Figure 2 schematically represents the procedure for projecting each Eigen face into feature space and assembling the KNN cluster for P persons.

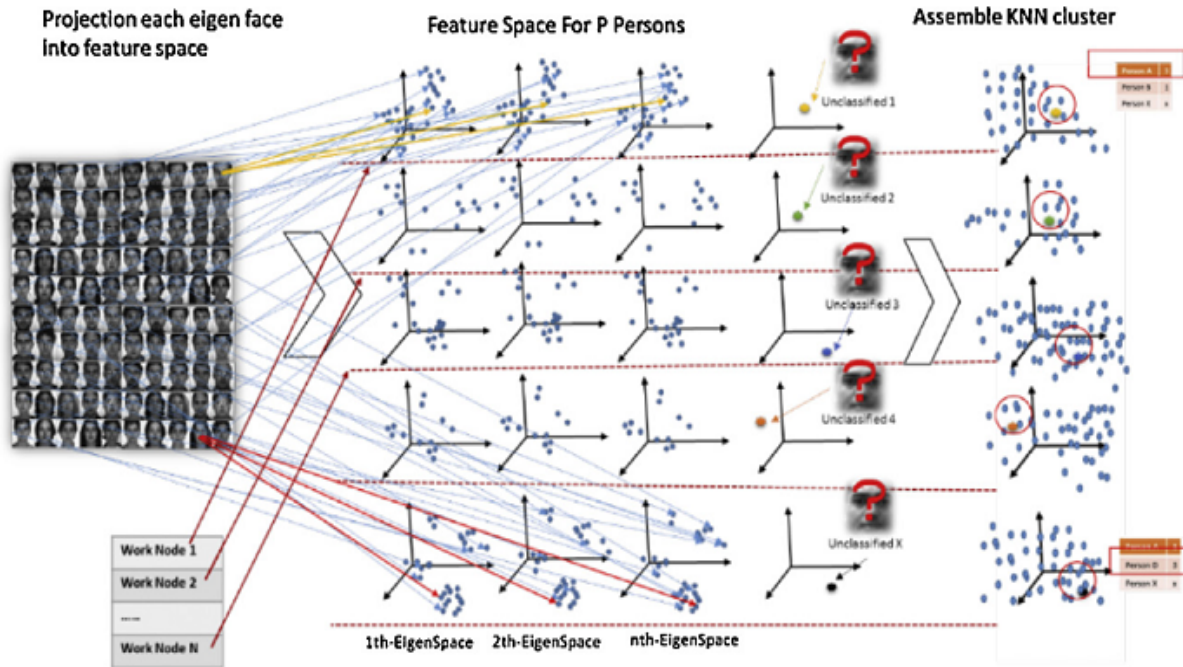


Figure 2: Procedure for projecting each Eigen face into feature space and assembling the KNN cluster.

The vector V_{ij} is one of the feature vectors Ω_i which is the projected vector in that face space. This is defined as the threshold to indicate the maximum allowable distance from the face space. For each test image, one gets $\phi = \zeta * P$ distance values. By applying the KNN algorithm, K nearest neighbors from ϕ can be chosen denoted as $K \ll \phi$, where $1 \leq K \leq (2\zeta - 1)$ is the proper range for K . Then, the occurrence for each class appearance in K is counted. More the occurrences in K , greater are the likelihood for the test image to get belong to that class. However, the selection of an appropriate K for this algorithm is the key issue. The larger K value reduces the effects of noise, but makes the boundaries between the classes less distinct. Thus, choosing a suitable K is essential to improving the classification accuracy.

4. K-Nearest Neighbor Classifier

The KNN classifier is an extension of the simple NN classifier system, which works on the basis of nonparametric decision. Each query image is examined based on the distance of its features from that of the training images [19]. Thus, the NN is the image having the minimum distance from the query image in the feature space. The distance between the two features is measured with respect to four distance functions such as City block, Euclidean, Mahalanobis, and the Direction Cosine. The KNN algorithm uses the K closest samples to the test image, where each of them belongs to a known class C_i . The test image is categorized in the class C_i , which has the majority of the occurrences among the K samples. The performance of the KNN classifier is decided by the K values and the topological distribution of training samples over the feature space. The JPEG images of (40×45) pixels are converted into a vector of 1800 elements, describing a point within 1800-dimensional image space. By measuring

the distance between these points, an indication of image similarity is obtained. Similar images are located close together, while dissimilar images are spaced far apart within the image space. Then, the KNN algorithm is implemented in the MapReduce environment as illustrated in Figure 3.

After Eigen-decomposition in the feature extraction phase, the feature package for each set of training images are gathered including the face space, mean image, and feature vectors given by:

$$i = [E_i, \bar{X}_i, \Omega_i] \quad (7)$$

with these P feature packages $[\phi_1, \phi_2, \dots, \phi_1, \dots, \phi_p]$ forming the feature cluster \mathcal{C}

$$= [1, 2, \dots, i, \dots, p], 1 \leq i \leq p \quad (8)$$

It is used for the next MapReduce cycle. As the classification procedure begins, every working node gets ϕ from the feature database. Hadoop then begins delivering the subpart for whole test-image URLs to each working node. After each image URL is received by each working node, the mean image \bar{x}_i is subtracted and projected into each face space E_i . We can get the projected vector for class ψ_i , for class C_i and then calculate the distances between class vectors and the projected vector ψ_i . This step is the repeated for every class v_{ij} of Ω_i . Upon calculating all distance values have, they are assembled as a KNN cluster before being sorted in ascending order. Finally, majority voting is applied from this K-nearest neighbor to determine the class label of the test image and for tagging it accordingly. The procedure described above is repeated for all test images in each working node until all test images have been classified.

5. Overall Architecture

5.1 Skeleton Diagram

Figure.3 depicts the division procedure of the face recognition. Some of the image sets are used for training and the rest are used for testing. Original images are not used because of two reasons namely the dimension curse and the diversity of the formats. The former is too high to build a robust recognition system and the later increases the rate of error identification significantly. After dimension reduction, the facial region is located to obtain face patches. This step is suitable for both the training and the testing images. Feature extractions are performed after preprocessing. The feature data (the face space, feature vectors, etc.) for each class is obtained using the assembly of KNN cluster by applying the KNN algorithm to each test image.

5.2 Detailed Workflow

The Hadoop's structure restricts the completion of the work in a single MapReduce cycle. This limitation is surmounted by dividing the whole process into minor and major steps as shown in Figure 4. These steps include (a) image-list scanning, (b) feature extraction, (c) recognition and, (d) classification.

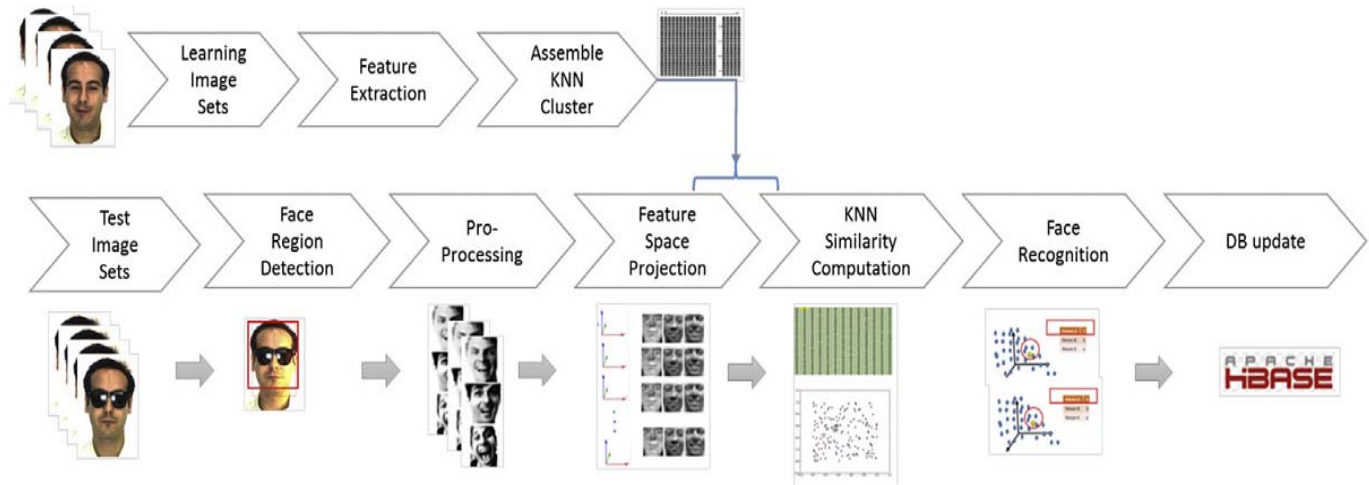


Fig.3. Facial image classification skeleton diagram

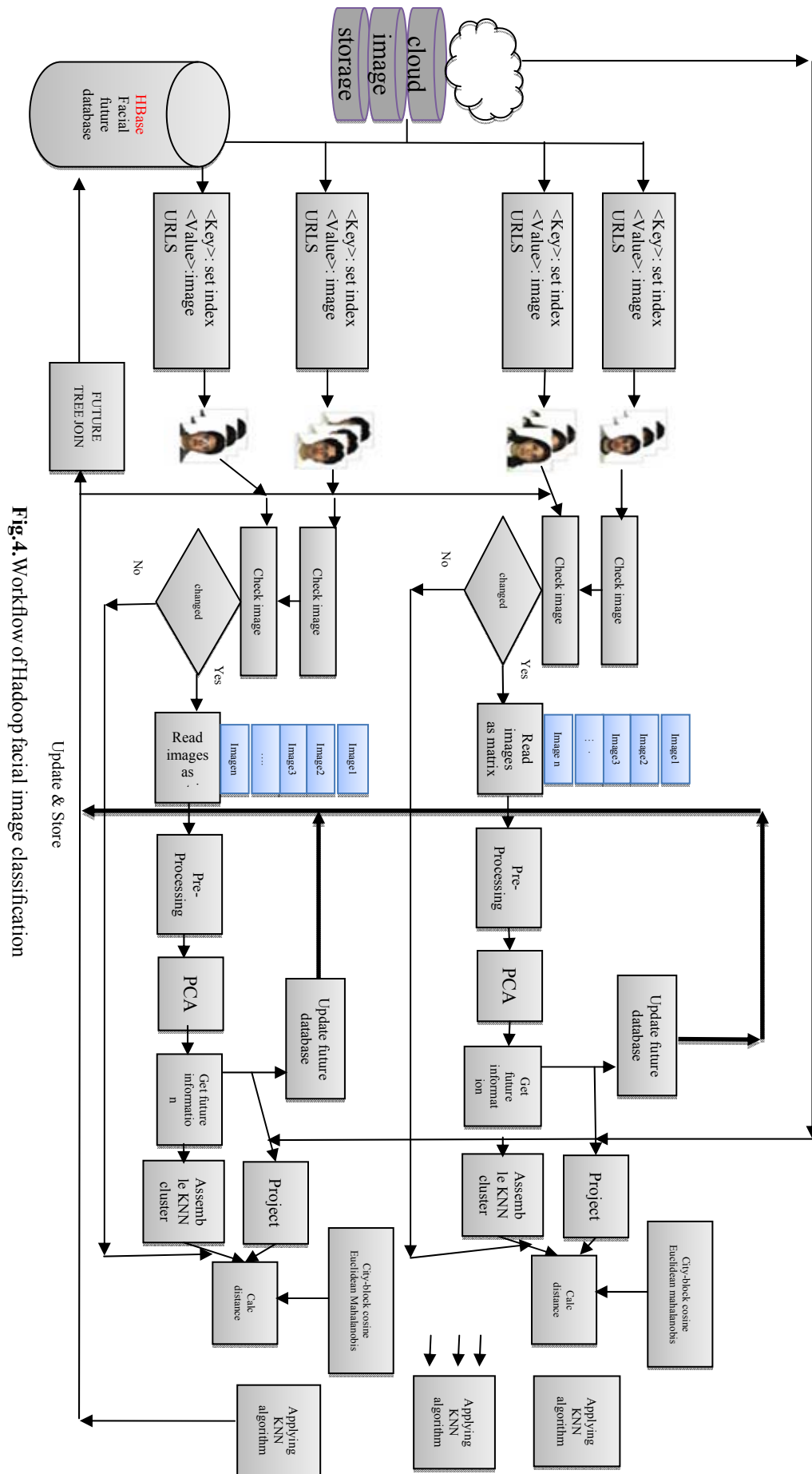


Fig.4. Workflow of Hadoop facial image classification

As aforementioned, Hadoop can read images as inputs. Firstly, the MapReduce step scans the image to get the image URLs for training and test images called Hadoop Image Processing Interface (HIPI) [20]. Sometimes, the image providers place the images in different locations. Consequently, each working node scans some locations by mapper and then reducer puts them together to form a full URL list. In this way, Hadoop can process images indirectly using URLs. Second step extracts the facial features. For each set of training images, mapper reads the input URLs as images, converts RGB images into gray-scale, and crops the image to a manageable size depending on the RAM restriction. Section below discusses about the process of locating the facial region. Thirdly, a matrix is constructed and concatenated from each cropped gray-scale facial image. Subsequently, the mean image is subtracted for reduce processing. During reduce step, eigen-decomposition (with PCA) is performed on the input matrix, where the essential data feature is extracted from the input matrix to forming a feature package. Next, the acquired feature package is updated and stored in a feature database. Hence, the feature data can be reused.

Finally, the map/reduce step perform the recognition. Every working node acquires all feature packages following Eq. (8). Mapper reads different parts of the test images' URL to change into gray-scale and crops them to the proper size as training image. During reduction, as a new image data enters the reducer projects it into every face space. Thus, a projected vector of the corresponding face space is acquired. Then, the distance between the feature vectors and the projected vector is calculated. Various kinds of distance strategies are applied, where the KNN algorithm is applied to determine the first k-nearest neighbors and to count the occurrences for each class. The highest number of occurrences provides the largest probability that the image belongs to that class.

5.3 The Face Database

In the present work, the experiments are conducted using a database of 3120 images from 120 individuals (65 male, 55 female) from the AR Face Database provided by Martinez and Benevento [21]. Some of the images from each disjointed set are used as training images as displayed in Figure 5. Two FTPs as image providers are set up because Hadoop cannot process the image formats directly. However, the Hadoop image processing cluster can access each image through its URL.

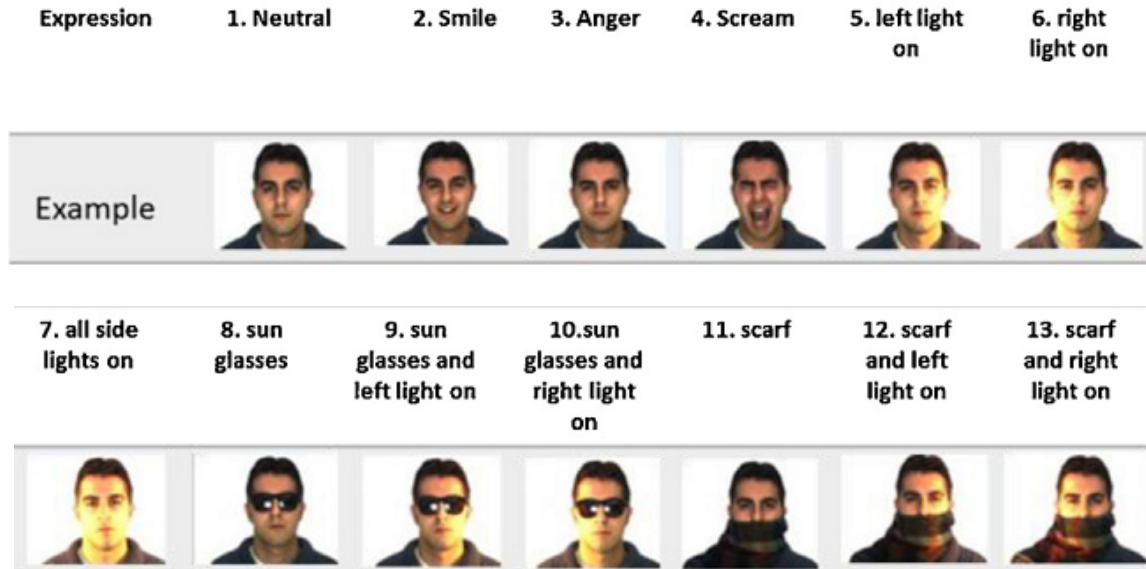


Fig. 5. Examples of training images.

5.4 Image Pre-processing

Figure 6 displays the amount of time consumed in PCA based image extraction and classification. A significant reduction in the error rates is observed by introducing an image preprocessing step to the Eigen face method for face recognition. Several categories of image preprocessing techniques exist such as color normalization, statistical methods, and convolution filters [22].

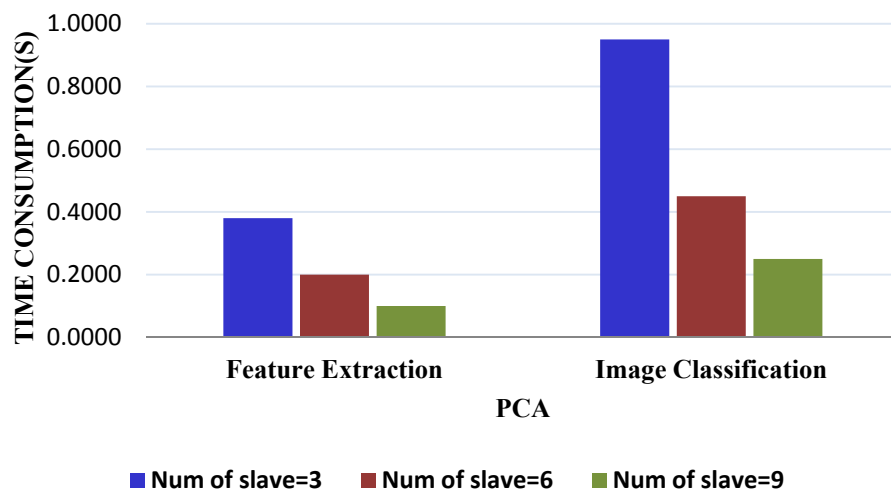


Fig.6. Processing time as a function of number of working nodes.

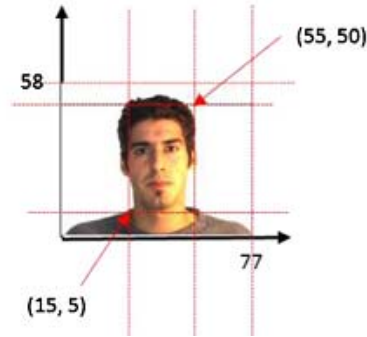


Fig.7. The cropping up process and dimension of the face region.

Following the standard procedure [22], each image is resized to a width and height of 77 and 58 pixels, respectively. The face region is cropped at (40×45) pixels to further improve the recognition rate and the cropped images are converted to gray-scale. Every additional 1 cm dimension in the facial area (not including the region below the chin) is found to produce merely 0.017 ± 0.002 recognition rates. Figure 7 depicts the cropping up procedure of the facial region with appropriate dimension.

6. Experimental Results

6.1 Number of Working Nodes Dependent Processing Time

The MapReduce assisted feature extraction performance and the processing time for image classification as a function of different numbers of working nodes are evaluated as illustrated in Figure 6. The average time expended is found to decrease noticeably with the increase of slave nodes number. Furthermore, the time consumption is decreased almost linearly as the number of working nodes is increased from three to nine. This reduction in time is attributed to the more parallelism induced effect with each new node. For instance, with only three working nodes in the MapReduce the PCA average is 0.3729 s per image during feature extraction and 0.9519 s per image during image tagging. Moreover, as the number of working nodes increased, the total processing time remarkably decreased sharply by about two third.

6.2 Number of Training Images Dependent Recognition Rate

Figure 8 depicts the effect of varying number of training images on the facial expression (neutral) recognition rate. Inclusion of more training images is found to considerably improve the recognition rate. The best recognition rate for neutral expression is achieved for eight training images. Conversely, for non-neutral facial expressions (Figure 5) such as a smile (Label 2), angry (Label 3), or scream (Label 4), and totally illuminated (Label 7) the best recognition rate is attained with six images instead of eight. For facial images covered by a scarf (Labels 11, 12, and 13), the recognition rate remained roughly the same even after increasing the number of training images. Interestingly, for images with sun-glasses (Labels 8, 9, and 10) the recognition rate did not decrease significantly at

all. In particular, Label 7 (in the presence of illumination from all sides) could not produce high recognition rate, which suggests that PCA is sensitive to light intensity.

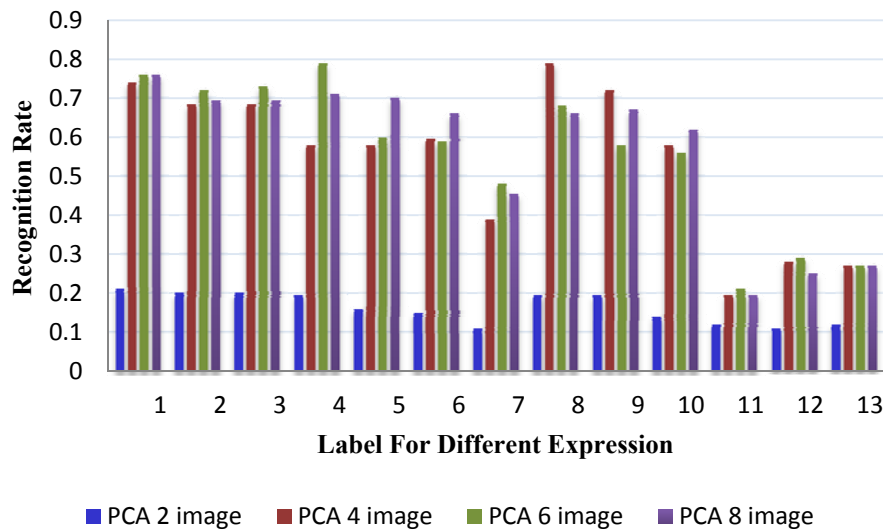


Fig.8. Number of training images dependent recognition rate.

6.3 KNN Number Dependent Recognition Rate

The experimental results on the KNN number dependent facial expression recognition rate (Figure 9) exhibited that it has insignificant impact on PCA. However, slight fluctuations in the recognition are evidenced for larger K values. This is because as the value of K increases, more data risks enter the 'counting region', resulting miss-classification.

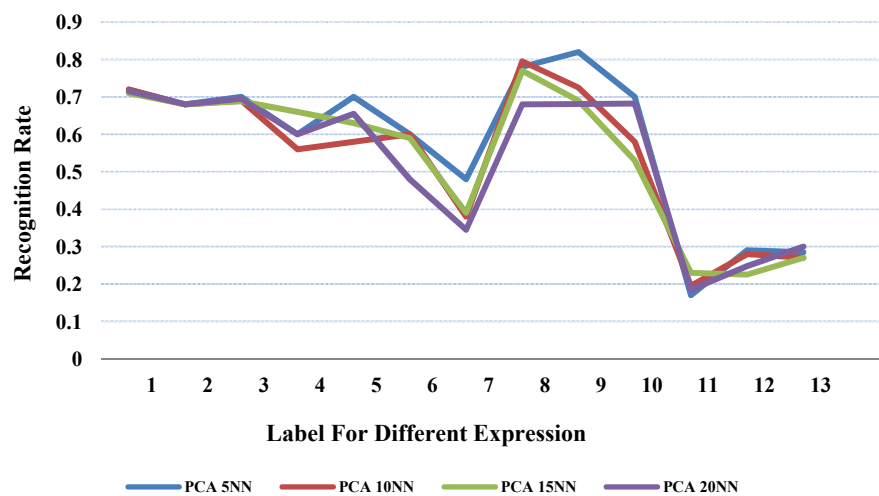


Fig. 9. KNN number dependent recognition rate.

6.4 Recognition Rate Using Varying Distance Strategies

Mahalanobis distance strategy is used to determine the recognition rate for neutral expressions (Figure 10), which produced the best result all together. The cosine strategy achieved the best results for Labels 2, 3, and 4, and the Euclidean strategy attained good results for the rest. However, extreme lighting (Label 7) is found to be detrimental for the recognition rate. Meanwhile, for Labels 11, 12, and 13, the recognition rates dropped sharply. Besides, the covered or partially obscure face continued to plague the PCA algorithms.

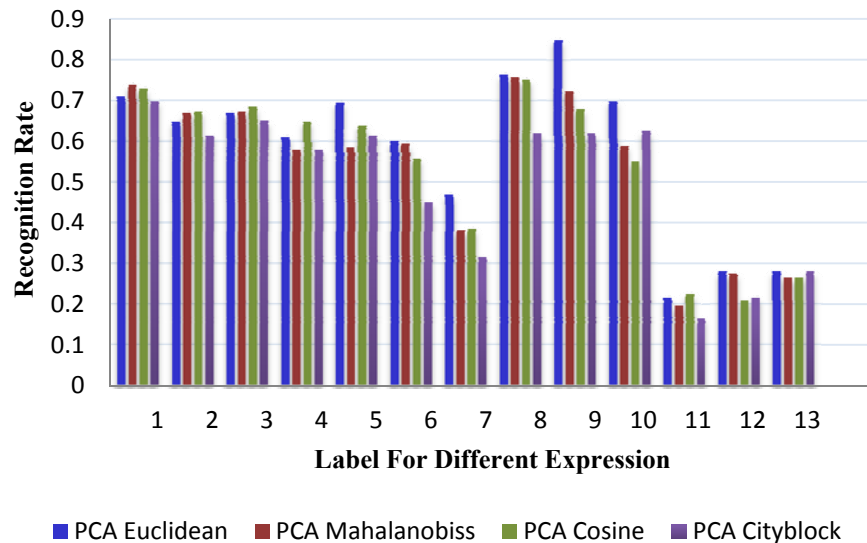


Fig.10.Recognition rate using different distance strategy

7. Conclusion

We proposed a new MapReduce based KNN algorithm using the Hadoop platform for efficient and accurate recognition of facial expressions. Following Martinez and Benevento, 3120 images from 120 individuals (65 male, 55 female) are selected from the AR Face Database and the experiments are carried out. The feature extraction performance and the processing time for image classification are determined by varying the numbers of working nodes. KNN number dependent facial expression recognition rate displayed slight influence on PCA. The achieved processing time of the present algorithm is demonstrated to be superior than the one obtained using traditional methods. Furthermore, the recognition rate under different situations with PCA and Mahalanobis distance strategy produced excellent facial images recognition for neutral expression. It is asserted that fully illuminated and covered face continues to be a challenge for PCA based face recognition algorithms. Moreover, the recognition rate is not significantly affected for images wearing sun-glasses. This observation may contribute towards the development of proficient and perfect facial appearances recognition algorithm and modeling useful in computer graphics.

REFERENCES

- [1] P. Fin de Carrera, Face Recognition Algorithms. Ion Marqu'es, Proyecto Fin de Carrera, 2010, June 16.
- [2] Y.M. Mustafah, A. Bigdeli, A.W. Azman, B.C. Lovell, An automated face recognition system for intelligence surveillance: smart camera recognizing faces in the crowd, in: IEEE International Conference on Distributed Smart Cameras, 2007, pp.147–152.
- [3] O. Arandjelovic, R. Cipolla, A Face Recognition System for Access Control using Video, Department of Engineering, University of Cambridge, Cambridge, UK, 2005, December.
- [4] H.R. Chennamma, L. Rangarajan, Mugshot identification from manipulated facial images, *Int. J. Mach. Intell.* 4 (1) (2012) 407.
- [5] F. Abdat, C. Maaoui, A. Pruski, Human–computer interaction using emotion recognition from facial expression, in: IEEE, UKSim 5th European Symposium on Computer Modeling and Simulation, vol. 3, 2011, pp. 196–201.
- [6] F. Dornaika, B. Raducanu, Facial Expression Recognition for HCI Applications, IGI Global, 2009.
- [7] K. Beyer, J. Goldstein, R. Ramakrishnan, U. Shaft, when is nearest neighbor meaningful, in: The 7th International Conference on Database Theory, 1998, June, pp. 217–235.
- [8] L. Sirovich, M. Kirby, A low-dimensional procedure for the characterization of human faces, *J. Opt. Soc. Am.* 4 (1987) 519–524.
- [9] M. Turk, A. Pentland, Eigenfaces for recognition, *J. Cognit. Neurosci.* 3 (1) (1991) 71–86.
- [10] M. Turk, A. Pentland, Face recognition using Eigenfaces, *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Maui, Hawaii, USA, 1991, June, pp. 586–591.
- [11] G.W. Cottrell, M.K. Fleming, Face recognition using unsupervised feature extraction, *Int. Neural Network. Conf.* 3 (1) (2012) 181–185.
- [12] K. Kim, Face Recognition using Principle Component Analysis, Department of Computer Science USA, 2000, June.
- [13] M. Yamamoto, K. Kunihiro, Parallel image database processing with MapReduce and performance evaluation in pseudo distributed mode, *Int. J. Electra. Comm. Stud.* 3 (2) (2012) 211–228.
- [14] K. Potisepp, Large-Scale Image Processing using MapReduce, Faculty of Mathematics and Computer Science Institute of Computer Science Computer Science, 2013, May, pp. 29.
- [15] Intel Distribution for Apache Hadoop Software, Real-Time Video Surveillance Across Locations, Shanghai Ideal Information Industry (Group) Co. Ltd., 2013, March, pp. 1–2.
- [16] The Apache Hadoop Website (Online). Available: <http://hadoop.apache.org/>
- [17] D. Jeffrey, G. Sanjay, and MapReduce: simplified data processing on large cluster, in: OSDI'04 Proceedings of the 6th conference on Symposium on Operating System Design & Implementation, vol. 6, 2004, p. 10.
- [18] W. Zhao, R. Chellappa, A. Rosenfeld, P.J. Phillips, Face recognition: a literature survey, *ACM Comput. Survey* 35 (4) (2000) 399–458.
- [19] T.M. Cover, P.E. Hart, nearest neighbor pattern classification, *IEEE Trans. Inform. Theory* 13 (1) (1967) 21–27.
- [20] S. Chris, L. Liu, A. Sean, L. Jason, HIPI: A Hadoop Image Processing Interface for Image-based MapReduce Tasks, University of Virginia, Department of Computer Science, 2011 (B.S. thesis).
- [21] A.M. Martinez, R. Benevento, "The AR Face Database".CVC Technical Report vol. 24, 1998.
- [22] T. Heseltine, N. Pears, J. Austin, Evaluation of image preprocessing techniques for Eigen face based face recognition, *Proc. SPIE* 4875 (2002) 677–685.

Construction of S-Box Based on Mobius Transformation and Increasing Its Confusion Creating Ability through Invertible Function

M.Sarfraz ^{1*}, Iqtadar Hussain ², Fateh Ali ¹

¹Department of Mathematics and Statistics, Riphah International University Islamabad, Pakistan

²Department of Mathematics, King Khalid University, Abha, Saudi Arabia

Abstract-Construction of widely held nonlinear transformation recognized as substitution box(S-box) which is responsible for security of modern block ciphers. Also this non-linear constituent establishes resistance against differential and linear attacks, as a result the S-box increases the ability of confusion of the cipher during the process of encryption. We proposed an algorithm based¹ on specific category of Mobius transformation for the construction of secure S-box recognized as transformed S-box. Moreover this Mobius transformation relies on elements of $GF(2^8)$ which are generated through particular type of primitive irreducible polynomial. Afterwards, we apply invertible function on transformed S-box for increasing its confusion creating aptitude and for cryptographically resilient S-box. This article also incorporated the assessment of the strength of constructed S-box through the utilization of renowned cryptographic properties such as non-linearity, criteria for bits independence, strict avalanche criterion, bits independence for SAC, bits independence for non-linearity, differential approximation and linear approximation probabilities.

Index Terms-Invertible Function, Mobius Transformation, Substitution Box.

I. INTRODUCTION

In the present state, the whole world is very firmly enclosed by the sphere of the information epoch. The instant propagation of latest and fast technology of computers in the different sectors improved the value of encryption for different sectors, such as business dealings between commercial creativities, as well as for armed utilization. Also, in day-to-day utilization, it becomes essential because its compromise may result in economic loss, disclosure of commercial or martial confidential and even the mislaying of life. Cryptology has an exceptional ways of utilization of encryption capabilities to provide security of information.

S-box represent individual nonlinear component in many algorithms for creating confusion in the data [1] and consequently plays a vital role in their security. The confusion process is applied to create a complex connection between the encrypted data and the key. The confusion ability is also examining the conversion impact of a single bit or more input bits and relying of output bits [2-3]. There are two basically used block ciphers Feistel ciphers (DES) and S-P network, where Feistel ciphers creates 50% confusion in every round while SPN transforms the complete information. S-box plays a central role to create confusion during encryption to provide more security of confidential information [4-5]. For this purpose, a lot of researchers have shown their interests to construct secure S-

Corresponding Author: Muhammad Sarfraz, Riphah International University Islamabad, Pakistan.

Email: msarfraz1112@yahoo.com

boxes and to increase their confusion ability.

Substitution box is a nonlinear transformation which proceeds with some amount of input bits m and as a result converts these bits into some amount of output bits n but it's not necessary that input bits are equal to output bits [6]. The constitution of different S-boxes makes a decision about the confusion ability of the considered cipher. A $m \times n$ substitution box can be applied having 2^m elements and each element have m bits.

In this article, we present a technique for the construction of strong S-box and then increasing its ability of confusion creating. The proposed method is applied to increase the nonlinearity because nonlinearity represents the confusion creating ability of S-box. In this process, Mobius transformation (LFT) is formed with the help of action of $PGL(2, GF(2^8))$ on $GF(2^8)$ and to find elements of transformed S-box through Mobius transformation, elements of $GF(2^8)$ are utilized which are generated through primitive irreducible polynomial [7-8]. Similarly Invertible function is then used on each element of transformed S-box to increase confusion for cryptographically secure S-box. Furthermore, the strength of newly constructed transformed and modified S-boxes are analyzed through utilization of cryptographic properties, including differential approximation, linear approximation, nonlinearity test, independence of output bits and strict avalanche criterion [9-10]. Comparison is also made with other renowned S-boxes including APA [11], Skipjack [12], S_8 Liu J [3], Hussain [13] and Residue Prime [14] S-boxes.

This article is arranged as follows: Section 2 consists of brief discussion about methodology of generated elements of $GF(2^8)$ and an algorithm for the construction of transformed S-box. Application of invertible function on elements of transformed S-box and then construction of modified S-box to increase confusion ability is presented in Section 3. Section 4 deals with the comparison of strength of modified S-box with transformed S-box as well as with well-known S-boxes through cryptographic properties. Lastly, conclusion of paper is presented in Section 5.

II ALGORITHM FOR CONSTRUCTION OF TRANSFORMED S-BOX USING $PGL(2, GF(2^8))$

To design a transformed substitution box (S-box) we utilized a special form of Mobius transformation (LFT) and its application on Galois field $GF(2^n)$ where $n=8$ having elements from 0 to 255. To make use of transformation in the construction of transformed S-box through the action of $PGL(2, GF(2^8))$ on $GF(2^8)$ of order 256 [15], we have following designed Mobius transformation (LFT),

$$T: PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$$

$$T(t) = \frac{at + b}{ct + d}, \text{ where } a.d - b.c \neq 0 \text{ and } t, a, b, c, d, \in GF(2^8) \quad (1)$$

The construction of transformed S-box begins with the utilization of $GF(2^8)$ and with the use of action of $PGL(2, GF(2^8))$ on Galois field of order 256 gives the function $T(t)$. The solutions of $T(t)$ are the elements of $GF(2^8)$ to design the transformed S-box. It must be noted that the value of t belongs to $GF(2^8)$ from 0 to 255 and used in LFT after conversion into polynomials. An algorithm stops it's working if the condition $a \times d - b \times c \neq 0$ does not hold. Moreover, when we alter the values of t in numerator and denominator then there may be situation that result of denominator will be equal to zero. We also checked this value of t in an algorithm which makes denominator zero. To overcome this error of zero denominator, we assigned an appropriate remaining value at the

end to complete the elements of S-box. To calculate the values of $T(t)$, we operated individually on $((a)(t) + b)$ and $((c)(t) + d)$ after using transformed values from 0 to 255 of t, a, b, c and d into binary form. To operate on binary form easily we represented these values into polynomial form. The values of numerator and denominator of $T(t)$ are changed with corresponding binary values from Table 1, which are shown in the form of exponent of 'm'. Also 'm' is interpreted as the solution of the particular primitive polynomial represented in (2) such that

$$P(y) = y^8 + y^4 + y^3 + y^2 + 1 \quad (2)$$

$$P(m) = m^8 + m^4 + m^3 + m^2 + 1 = 0 \quad (3)$$

The $P(m)$ expressed in (3) is used to generate different elements of $GF(2^8)$. The construction of algebraic methodology for $GF(2^8)$ utilized in this work represented in Fig.1 and is defined as, $GF(2^8) = \frac{Z_2[y]}{\langle P(y) \rangle}$ where $Z_2 = \{0,1\}$ and $P(y) = y^8 + y^4 + y^3 + y^2 + 1$ [9]. Representation in terms of "m" and simplification methodology which gives elements of transformed S-box is explained in Table 2.

TABLE 1
REPRESENTATION OF GENERATED ELEMENTS OF $GF(2^8)$

$GF(2^8)$	Binary values	Decimal Form	$GF(2^8)$	Binary values	Decimal Form
0	00000000	0	m^{10}	01110100	16
m	00000110	21	m^{11}	11101000	232
m^2	00000110	15	m^{12}	11001101	105
m^3	00001000	8	m^{13}	10000111	235
m^4	00010100	18	.	.	.
m^5	00100000	32	.	.	.
m^6	01000000	64	.	.	.
m^7	10000010	28	m^{253}	01000111	71
m^8	00011101	39	m^{254}	10001110	152
m^9	00111010	68	m^{255}	00000001	1

TABLE 2
CONSTRUCTION OF THE TRANSFORMED S-BOX

$GF(2^8)$ (0 to 255)	$T(t) = \frac{(230)(t) + 33}{(93)(t) + 204}$	Here we are taking 'm' from Table 1	S-box elements
00000000	33/204	$m^{250}/m^{239} = m^{12}$	12
00000001	199/145	$m^{249}/m^{41} = m^{209}$	209
.	.	.	.
.	.	.	.
00000101	58/100	$m^{89}/m^{20} = m^{70}$	70
00000110	220/57	$m^{85}/m^{194} = m^{34}$	34

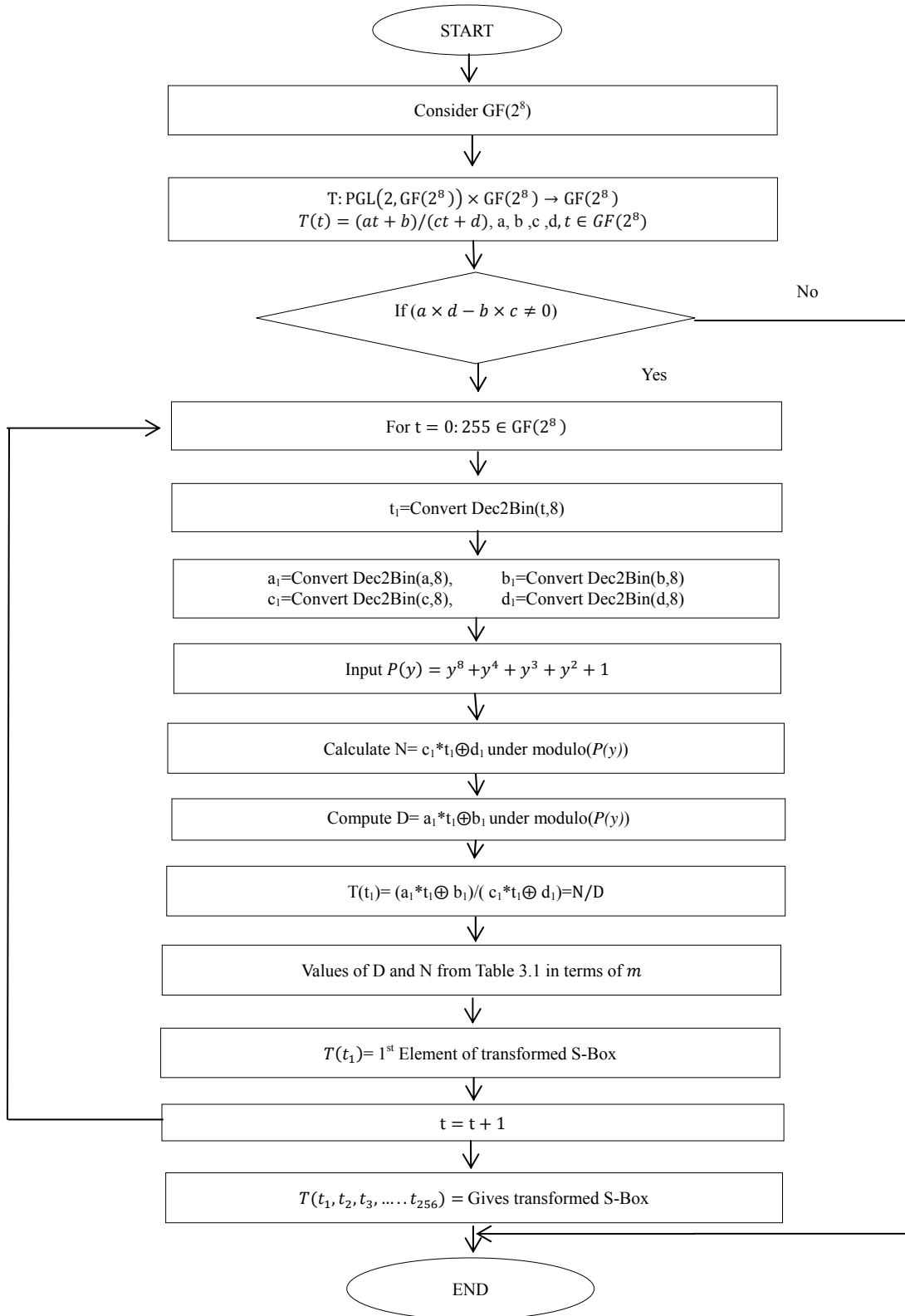


Figure 1. Algorithm for transformed S-box

TABLE 3
TRANSFORMED S-BOX IN THE FORM OF 16×16 MATRIX

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	209	214	22	205	218	24	252	64	52	226	63	38	107	229	102
1	61	203	4	211	42	130	123	83	191	194	143	166	10	86	13	136
2	152	132	129	167	3	122	116	184	244	55	21	232	223	2	156	173
3	17	230	151	112	120	195	6	51	201	50	29	33	89	104	180	240
4	108	236	103	172	147	239	158	146	213	186	247	5	188	251	1	198
5	74	197	124	200	44	67	16	19	127	87	80	168	254	206	7	149
6	37	54	208	242	233	189	155	221	26	94	88	207	43	81	78	58
7	225	30	106	121	177	181	160	9	159	204	15	90	98	59	235	193
8	187	32	85	141	202	72	117	250	171	40	68	253	163	91	154	95
9	28	14	41	66	162	84	35	82	219	109	148	179	161	153	137	53
10	11	245	237	46	11	131	150	255	145	238	76	217	165	75	192	222
11	176	140	97	36	100	185	20	224	27	92	231	133	105	139	249	96
12	115	56	119	47	212	142	170	39	215	93	138	8	69	125	178	23
13	157	73	57	49	31	62	101	246	128	175	126	48	144	169	196	182
14	243	18	135	45	248	134	227	65	210	60	79	199	164	228	220	99
15	114	216	71	0	77	234	118	183	241	190	25	110	174	113	70	34

TABLE 4
MODIFIED S-BOX IN 16×16 MATRIX

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	27	97	104	53	69	124	39	22	207	83	52	78	101	178	61	165
1	72	79	3	103	113	148	130	250	211	84	131	248	17	245	24	138
2	186	158	145	251	10	129	147	218	14	86	48	42	115	9	182	229
3	60	56	171	159	135	87	5	90	73	89	40	108	228	183	206	2
4	187	38	166	230	167	35	176	164	109	220	11	0	214	31	12	88
5	209	93	139	74	123	202	63	58	142	246	255	234	16	64	6	173
6	96	85	98	4	41	213	191	117	33	237	231	67	114	252	221	65
7	49	45	177	132	193	205	242	20	179	70	30	225	169	66	47	81
8	223	111	240	133	76	215	144	28	239	119	195	21	247	226	188	238
9	43	29	116	201	244	243	106	249	127	184	174	199	241	185	137	80
10	190	13	37	125	18	151	168	19	161	32	219	121	253	210	82	112
11	194	134	172	99	163	217	51	50	34	235	59	157	180	143	25	175
12	154	71	150	126	110	128	236	102	107	232	140	23	192	136	196	54
13	181	212	68	92	46	77	160	8	146	227	141	95	162	233	94	200
14	7	57	155	120	26	152	55	204	100	75	222	91	254	62	118	170
15	153	122	198	15	216	44	149	203	1	208	36	189	224	156	197	105

III CONSTRUCTION OF MODIFIED S-BOX

The structure of modified S-box depends upon the invertible function which is applied on elements of transformed S-box to shuffle the elements of S-box. The invertible function h utilized for the process of construction of modified S-box is organized in following steps,

Step I: Consider an invertible function $h(t) = mt + n$, for $m \neq 0$ and $m, n, t \in GF(2^8)$

Step II: Utilize particular instances $m = 3$ and $n = 15$, then function $h(t)$ becomes

$$h(t) = 3t + 15, \text{ where } 3, 15, t \in GF(2^8) \quad (4)$$

Step III: Transform t from transformed S-box.

Step IV: Generate elements of modified S-box using arithmetic modulo $P(y)$.

Shuffling of elements of transformed S-box through invertible function is represented in rows and columns form as 16×16 matrix signified in Table 4.

IV ANALYSIS OF MODIFIED S-BOX AND THEIR COMPARISON

4.1. Nonlinearity Comparison

Non-linearity represents the amount of bits that necessarily altered to reach the affine function which is at minimum distance. So for a large 'm' this computation will be difficult. Let us denote the series of a function f on F_2^n with α , then the non-linearity of f is defined as follows:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{i=0,1,\dots,2^n-1} \{|\langle \alpha, l_i \rangle|\} \quad (5)$$

Where l_i represent the i^{th} row of Hadamard matrix B_n .

Hadamard matrix B_n can be represent as follows,

$$B_n = \begin{pmatrix} B_{n-1} & B_{n-1} \\ B_{n-1} & -B_{n-1} \end{pmatrix}, B_0 = [1] \text{ and } n = 1, 2, 3, 4 \dots \quad (6)$$

To compute the nonlinearity when we consider substitution boxes in Galois Field of order 256 (i.e. $GF(2^8)$), where $n=8$) the nonlinearity of S-boxes must satisfies the relation $N_f = \frac{2^n - 2^{n/2}}{2} = 120$, when $n=8$ [16]. The value 120 of nonlinearity of f is computed as ideal value of S-box.

From Table 5, we observed that the minimum nonlinearity of modified S-box is equal to 106, which is greater when compared to the minimum nonlinearity of [3,12,13,14] S-boxes. Also invertible function increases the average nonlinearity of S-box from 106.75 to 108, which exhibit that application of invertible function has ability to increase the confusion creating strength of S-box. Furthermore, nonlinearity of modified S-box is greater when compared with Skipjack, S_8 Liu J, Hussain and Residue Prime S-boxes. Difference of nonlinearity can be seen in Fig. 2.

4.2 Strict Avalanche Criterion (SAC)

If an average result of output bits must be change to 0.5 when a single input bit j is complemented then given transformation display an avalanche effect. Any given function takes good avalanche effect if this process is repeated for each input bits j and 50% of the avalanche variables attain the values 1 [17].

Substitution box fulfills the property of SAC if only one input bit change then as a result half amount of output bits change. It must be noted that when we utilized substitution box to build a substitution-permutation (S-P network), then alteration of only one input bit causes an avalanche of variations. If for a function f the expression $f(x) \oplus f(x \oplus \alpha)$ is stable for all sequences α such that the weight of $\alpha = 1$, then the function $f : F_2^n \rightarrow F_2$ fulfills the condition of SAC [18].

Strength variation of SAC between designed S-boxes and renowned S-boxes is shown in Table 6 and graphically represented in Fig.3.

By considering the maximum values, minimum values, average values and square deviation values from Table 6, it's observed that square deviation of the newly constructed modified S-box is 0.017 and more acceptable than square deviation of Skipjack and Residue Prime S-boxes. Also the average value of SAC is comparatively better and ~ 0.5 .

TABLE 5
ASSESSMENT OF NONLINEARITY OF MODIFIED S-BOX

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Avg.
Transformed S-box	106	106	106	108	106	108	106	108	106.75
Modified S-box	106	110	108	108	106	110	106	110	108
APA S-box [11]	112	112	112	112	112	112	112	112	112
Skipjack S-box [12]	104	104	108	108	108	104	104	106	105.75
S_8 Liu J S-box [3]	105	105	104	100	107	105	106	107	104.875
Hussain [13]	104	100	108	106	102	106	104	108	104.75
Residue Prime [14]	94	100	104	104	102	100	98	94	99.5

Modified S-box (Minimum value=106, Maximum value=110, Average value=108)

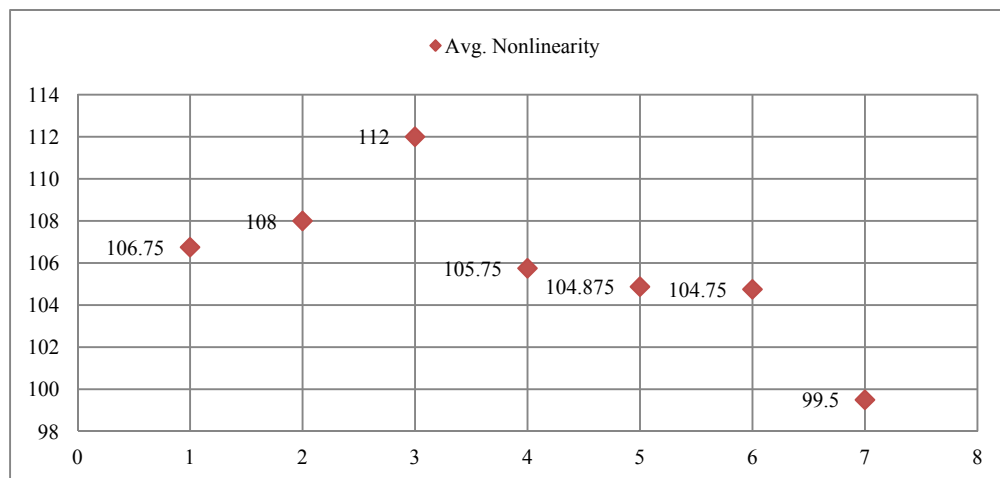


Figure 2. Comparison of Nonlinearity with S-boxes

TABLE 6
COMPARISON OF STRICT AVALANCHE CRITERIA FOR S-BOXES DESIGNED IN THIS WORK.

S-boxes	Max. value	Min. value	Avg. value	Sq. deviation
Transformed S-box	0.59	0.406	0.501	0.02
Modified S-box	0.59	0.421	0.497	0.02
APA S-box	0.56	0.437	0.5	0.016
Skipjack S-box	0.59	0.39	0.53	0.024
S ₈ Liu J S-box	0.59	0.429	0.499	0.017
Hussain	0.59	0.391	0.49	0.02
Residue Prime	0.67	0.343	0.51	0.032

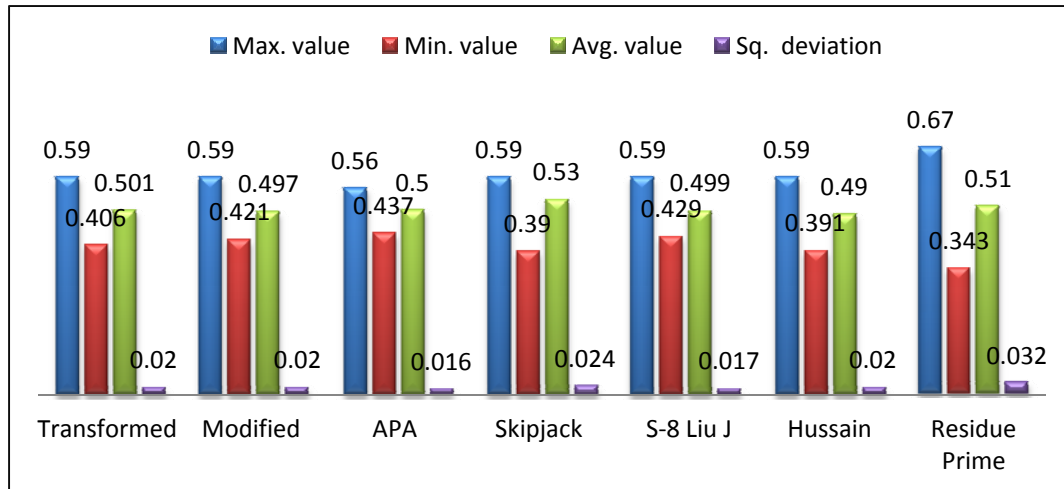


Figure 3. Comparison of Strict Avalanche Criterion

4.3 Bit Independence Criterion (BIC)

This is one more type of criterion for S-box to measure the strength which defined as the output bits y and z must be change individually whenever every single input bit x is given for all x , y and z . A bits independence criterion is appropriate property for every cryptographic scheme which was presented by Webster and Tavares [18]. In Reference [18] it is discussed that for the Boolean functions f_y, f_z ($y \neq z$) of two different output bits of substitution box, if the substitution box met bits independence criterion, $f_y \oplus f_z$ ($y \neq z, 1 \leq y, z \leq n$) must be exceptionally nonlinear and come nearby as possible to satisfy the strict avalanche criteria. Hence, we can also attest the bits independence by assessing the nonlinearity and strict avalanche criteria of $f_y \oplus f_z$.

For comparison of BIC for SAC between under consideration S-boxes we inspect average value, minimum value, and square deviation values which are appeared in Table 8 and their behavior represent that the average value and square deviation of modified S-box are 0.502 and 0.16 respectively which are better than the value of transformed S-

box. Analysis comparison of BIC for nonlinearity from Table 7 and Fig.4 represents that the average value is superior to the Skipjack, S_8 Liu J, Hussain and Residue Prime S-boxes.

TABLE 7
ASSESSMENT OF BIC FOR NONLINEARITY OF S-BOXES

S-boxes	Min. value	Avg. value	Sq. deviation
Transformed S-box	102	106.571	2.61081
Modified S-box	100	105.286	2.57539
APA S-box	112	112	0
Skipjack S-box	102	104.14	1.767
S_8 Liu J S-box	99	104.786	2.659
Hussain	100	105.071	2.17
Residue Prime	94	101.71	3.53

TABLE 8
ASSESSMENT OF BIC FOR SAC OF MODIFIED S-BOX

S-boxes	Min. value	Avg. value	Sq. deviation
Transformed S-box	0.459	0.498	0.17
Modified S-box	0.48	0.502	0.16
APA S-box	0.472	0.499	0.01
Skipjack S-box	0.464	0.499	0.018
S_8 Liu J S-box	0.468	0.489	0.016
Hussain	0.476	0.500	0.0137
Residue Prime	0.47	0.502	0.017

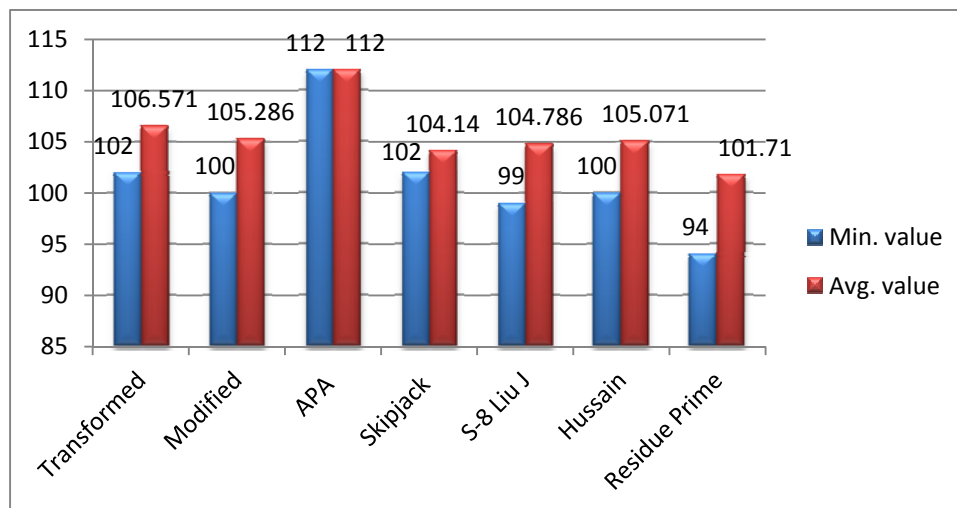


Figure 4. Comparison of BIC for Nonlinearity of S-boxes

4.4 Linear Approximation Probability (LP)

It is defined as the highest value of disparity of an occurrence. The uniformity of the input bits must be identical to the uniformity of the output bits. At the input level each i^{th} input bit is examined independently and its consequences are observed in the output bits.

As stated by Matsui's in his definition [19], the LPs of a substitution box is expressed as,

$$LP = \max_{\varphi(x), \varphi(y) \neq 0} \left| \frac{\text{Number of } \{x \in X / x. \varphi(x) = S(x). \varphi(y)\}}{2^m} - \frac{1}{2} \right| \quad (7)$$

where 2^m indicates the amount of elements belongs to the constructed substitution box and the collection of each feasible inputs bits to the substitution box are denoted by X . As well $\varphi(x)$ and $\varphi(y)$ represents the input/output masks correspondingly.

Assessment of LP of S-boxes are represented in Table 9 and graphical comparison is displayed in Fig.5 which have shown that before and after application of invertible function maximum value of LP=160 and maximum LP=0.125 i.e. there is no variations due to particular invertible function. Analysis comparison indicates that behavior of modified S-box against linear attacks is better when compare to Residue prime S-box and identical to Hussain S-box. Value of LP represents that transformed S-box maintains its resistance against linear cryptanalysis after application of invertible function.

TABLE 9
ASSESSMENT OF LP OF MODIFIED S-BOX

S-boxes	Transformed	Modified	APA	Skipjack	S ₈ Liu J	Hussain	Residue Prime
Maximum LP	0.125	0.125	0.062	0.109	0.105	0.125	0.132
Maximum value	160	160	144	156	159	160	162

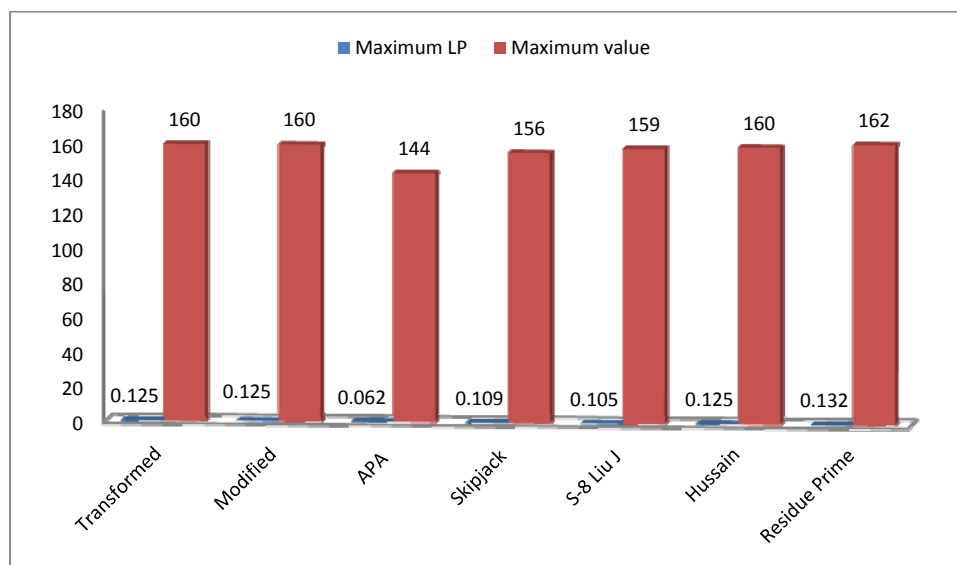


Figure 5. Comparison of LP of S-boxes

4.5 Differential Approximation (DP)

The substitution box is considered as the non-linear constituent during encryption of confidential information or data. In perfect situations, the substitution box indicates differential consistency. Δx is considered as input differential and Δy indicated as output differential. In order to make sure the differential consistency then Δx at the input level needs to distinctive map to an output Δy . In this technique of DP, it is noticed, how much probability that differential of input bits is individually mapped on differential at output bits. An input differential Δx must individually map to an output Δy [20]. To calculate differential uniformity, the DP of a specified substitution box can be stated as:

$$DP_{(\Delta x \rightarrow \Delta y)} = \left[\frac{\text{Number of } \{x \in X / S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n} \right] \quad (8)$$

Where X represents the set of very feasible input values and their numbers of elements are denoted by 2^n .

Comparison results of DP with famous S-boxes that are presented in Table 10 indicate that the strength of modified S-box against differential attacks is reasonable and also superior when compared to Residue Prime and Hussain S-boxes from literature. Graphical comparison is also represented in Fig.6.

Analysis of differential approximation probability of transformed and modified S-boxes represents maximum DP=0.0625 i.e. there is no variations due to particular invertible function $h(t)$ because transformed S-box maintain its maximum differential probability 0.0625 which is acceptable value for resistance against differential attacks.

TABLE 10
DIFFERENTIAL APPROXIMATION PROBABILITY ANALYSIS

S-boxes	Transformed	Modified	APA	Skipjack	S_8 Liu J	Hussain	Residue Prime
Max. DP	0.0625	0.0625	0.0156	0.0468	0.0390	0.125	0.281

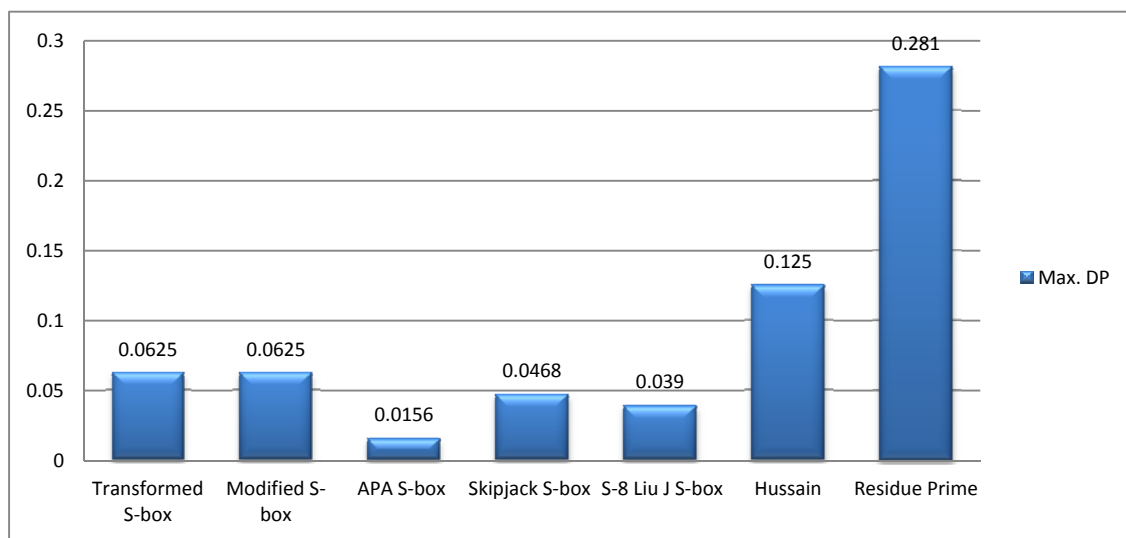


Figure 6. Comparison of DP of S-boxes

V. CONCLUSION

Substitution box is the most significant constituent in the encryption algorithms, combine in the substitution-

permutation network (SPN) to play a vital role. In this thesis, we have introduced a method for constructing strong S-box is established due to the action of $PGL(2, GF(2^8))$ on field $GF(2^8)$. These innovative generated S-box relates to a special form of Mobius transformation $(230t+33)/(93t+204)$. The additional benefit of the designed algorithm is that a large number of substitution boxes can be produced through the utilization of different elements of Galois field $GF(2^8)$ in linear fractional transformation. It is observed from the critical analysis that representation mechanism of the transformed S-box is straight forward and easy for software and hardware application.

Moreover, to investigate the encryption ability of transformed substitution box, the transformed S-box occupies all of the nonlinearity test, bit independence and strict avalanche criterions, which are more indispensable properties for resilient substitution boxes to increase confusion in the encryption procedure. We apply a particular type of invertible function to increase confusion ability of S-box and made comparison through important cryptographic properties. Also we have observed that application of invertible function increases the nonlinearity from 106.75 to 108 which specified that it has also increased confusion creating strength of S-box. We also made comparison of linear approximation (LP) and differential approximation (DP) probabilities which shows that the constructed S-box has acceptable resistance against linear and differential attacks.

A study is accomplished to associate the generated substitution box with important renowned substitution boxes and shows good results. So we conclude that we can utilize the generated S-box in block cipher to secure our confidential information during communication.

REFERENCES

- [1] Shannon, Claude E. "Communication theory of secrecy systems*." Bell system technical journal 28.4, 656-715 (1949).
- [2] Meier, Willi, and Othmar Staffelbach. "Nonlinearity criteria for cryptographic functions." Advances in Cryptology—EUROCRYPT'89. Springer Berlin Heidelberg, 1990.
- [3] Hussain, Iqtadar, et al. "Construction of S 8 Liu J S-boxes and their applications." Computers & Mathematics with Applications 64.8, 2450-2458 (2012)
- [4] Coppersmith, Don. "The Data Encryption Standard (DES) and its strength against attacks." IBM journal of research and development 38.3, 243-250 (1994)
- [5] Daemen, Joan, and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.
- [6] Nyberg, Kaisa. Advances in Cryptology-EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31-June 4, 1998, Proceedings. Vol. 1403. Springer Science & Business Media, 1998.
- [7] Hansen, Tom, and Gary L. Mullen. "Primitive polynomials over finite fields." Mathematics of Computation 59.200, 639-643(1992)
- [8] Hussain, Iqtadar, et al. "A projective general linear group based algorithm for the construction of substitution box for block ciphers." Neural Computing and Applications 22.6, 1085-1093 (2013)
- [9] Hussain, Iqtadar, et al. "Construction of new S-box using a linear fractional transformation. World Appl. Sci. J 14.12, 1779-1785 (2011)
- [10] Hussain, Iqtadar, et al. "Analyses of SKIPJACK S-Box 1." (2011).
- [11] Cui, Lingguo, and Yuanda Cao. "A new S-box structure named Affine-Power-Affine" International Journal of Innovative Computing, Information and Control 3.3, 751-759(2007)
- [12] Kim, Jongsung, and Raphael C-W. Phan**. "Advanced differential-style cryptanalysis of the NSA's skipjack block cipher." *Cryptologia* 33.3, 246-270 (2009)
- [13] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan and H. Mahmood, A group theoretic approach to construct cryptographically strong substitution boxes, *Neural Comput.*, doi:10.1007/s00521-012-0914-5, 2012.
- [14] Hussain, Iqtadar, et al. "Some analysis of S-box based on residue of prime number." *Proc. Pak. Acad. Sci* 48.2, 111-115 (2011)

- [15] Hussain, Iqtadar, et al. "Construction of cryptographically strong 8×8 S-boxes." World Applied Sciences Journal 13.11, 2389-2395 (2011)
- [16] D. Feng and W. Wu, Design and analysis of block ciphers, Tsinghua University Press, 2000.
- [17] Webster, A. F., and Stafford E. Tavares. "On the design of S-boxes." Advances in Cryptology—CRYPTO'85 Proceedings. Springer Berlin Heidelberg, 1986.
- [18] Mar, Phyu Phyu, and Khin Maung Latt. "New analysis methods on strict avalanche criterion of S-boxes." World Academy of Science, Engineering and Technology 48, 150-154 (2008).
- [19] Matsui, Mitsuru. "Linear cryptanalysis method for DES cipher." Advances in Cryptology—EUROCRYPT'93. Springer Berlin Heidelberg, 1994.
- [20] Biham, Eli, and Adi Shamir. "Differential cryptanalysis of DES-like cryptosystems." Journal of CRYPTOLOGY 4.1, 3-72 (1991).

SDN in Cellular Network and Implementation Challenges

Md. Humayun Kabir, Department of Computer Science & Engineering, University of Rajshahi, Rajshahi, Bangladesh

Abstract- Cellular data traffic has exploded in recent years, in large part due to the rapid proliferation of cellular devices such as smart phones, tablets and other Machine-to-Machine devices. New cellular technologies, like Long Term Evolution, have helped cellular providers to keep up with the traffic growth by increasing their radio access capacity. Although, it was a change in the right direction, the result appears to provide somewhat constrained enhancements in terms of reduction in complexity and improvement in flexibility. Software defined networking can simplify network management, while enabling new services. However, supporting many subscribers, frequent mobility, fine-grained measurement and control, and real-time adaptation introduces scalability challenges that future SDN architectures should address. In this article, various architectural aspects of today's and future SDN-based cellular network as well as its implementation challenges have been done.

Key words- SDN, OpenFlow, LTE.

I. INTRODUCTION

Everyday new technology, policies and smart devices are emerging, today's networking concept is also developing accordingly. The traditional network infrastructure is considered as a single system made by many physical elements, such as routers, switches, and firewalls on which the whole network controlling activities depend for communication and services. A single modification in any part of the network can increase the maintenance effort on the whole network, and sometimes it may cause a miscarriage of the total network. At present, most of the information technology (IT) related people identify the traditional networking paradigm as very much static and think it requires a lot of effort to physically change and laboriously organize and legalize the network [1].

Software Defined Networking (SDN) is a new approach in the networking paradigm that has given the idea to deal efficiently with the emerging network and to better handle the major growth in data traffic, network virtualization, and mobility of user equipment [2] [3]. SDN generally permits network administrators/operators to regulate their network systems programmatically, serving them to improve capabilities and scale without compromising performance, reliability, or user experience [4].

A traditional network layout (shown in Fig. 1) as it compares to an SDN network layout (shown in Fig. 2) [5] is described in the following. Traditional networking devices are composed of an embedded control plane that manages switching, routing and traffic engineering activities while the data plane forwards packet/frames based on traffic [6]. Here control plane is responsible to control the traffic related activities and data plane works as the traffic carrier. The control plane provides information used to build a forwarding table. The data plane consults the forwarding table to make a decision on where to send frames or packets entering the device. The networking device contains both of these planes and these are usually placed as built-in on the device [7].

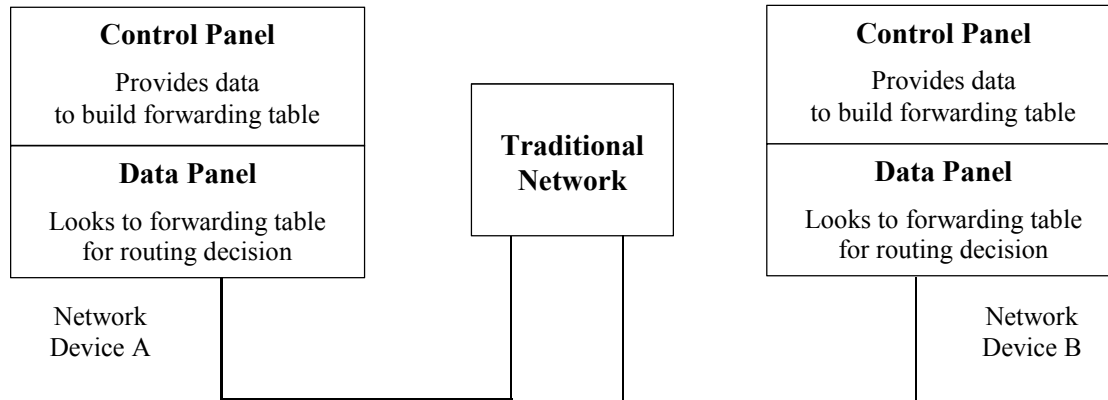


Figure 1. Traditional network layout

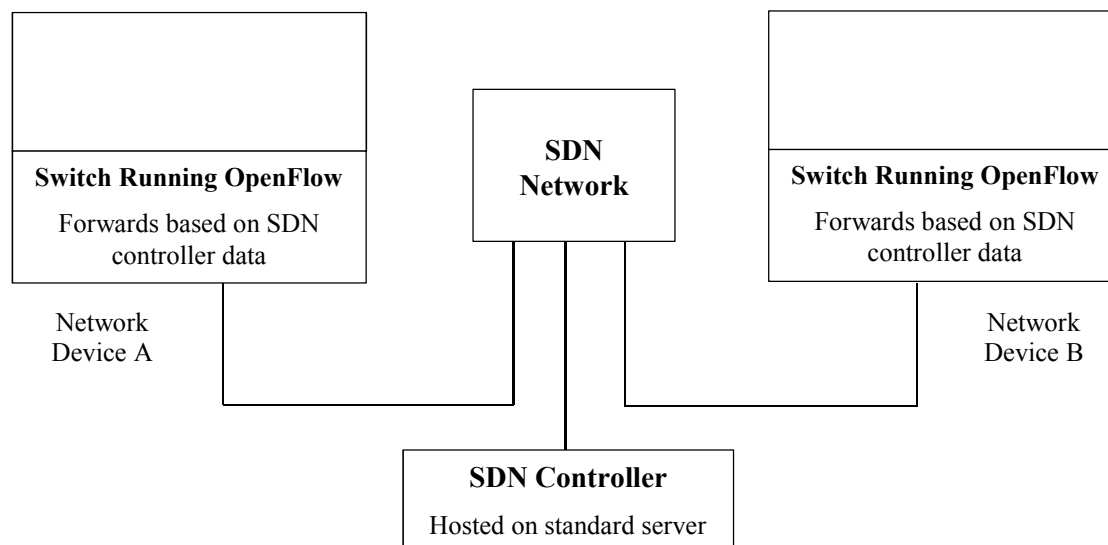


Figure 2. SDN network layout

In SDN architecture, control plane functions are removed from individual networking devices and hosted on a centralized server [8]. The SDN controller usually is an operating system with necessary SDN software. The controller generally communicates with the switch data plane through a protocol that is publicly known as OpenFlow [9]. OpenFlow transmits the instructions and commands to the data plane so that the data plane can forward the data to the right direction. To support the services the network devices must contain and run the OpenFlow protocol.

In this paper, various features about the architecture of today's and future SDN-based cellular network have been analyzed, and at the same time the implementation challenges of SDN to future cellular network are provided. The rest of the paper is organized as follows: section 2 briefly describes about the architecture of a generic cellular system, an overview of today's LTE cellular network architecture is demonstrated in section 3 and the limitations of today's cellular network is demonstrated in section 4; SDN overview is described in section 5, section 6 depicts a general architecture of SDN-based future cellular network, some recently published proposals for SDN-based

cellular network architecture are discussed in section 7, implementation challenges of future SDN-based Cellular Network are focused in section 8 and finally section 9 concludes the paper.

II. BASIC CELLULAR NETWORK ARCHITECTURE

The architecture of a generic cellular system [10] is described in Fig. 3. The schematic is not particular to a specific standard; rather it provides an idea of the different components in the network. In the radio access subsystem, the mobile station (MS), sometimes called user equipment (UE) is the device whose position is to be determined. Base stations (BSs – also called eNodeBs) are fixed transmitters that are points of access to the rest of the network. A MS communicates with a BS during idle periods (signaling), cellular phone calls (voice) or other data transmission. Base stations are controlled by radio network controllers (RNCs) that also manage the radio resources of each BS and MS (frequency channels, time slots, spread spectrum codes, transmit powers, and so on).

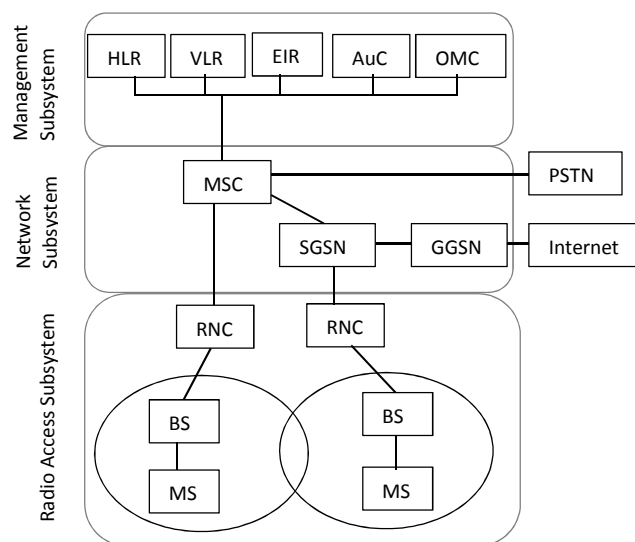


Figure 3. Generic cellular network architecture

The network subsystem carries voice and data traffic and also handles routing of calls and data packets. The mobile switching center (MSC) and the serving and gateway GPRS (General Packet Radio Service) support nodes (SGSN and GGSNs) are responsible for handling voice and data respectively. These network entities perform the task of mobility management; they keep track of the cell or group of cells where a MS is located and handle routing of calls or packets when a MS performs a handoff. They connect to the public switched telephone network (PSTN) or the Internet. Several databases in the management subsystem, such as home location register (HLR), visitor location register (VLR), equipment identity register (EIR), authentication center (AuC), operations and maintenance center (OMC), are used for keeping track of the entities in the network that are currently serving the MS, security issues, accounting and other operations as shown in the upper part of Fig. 3.

III. TODAY'S LTE CELLULAR NETWORK ARCHITECTURE

Long Term Evolution (LTE) cellular networks connect base stations (eNodeB) to the Internet using IP networking equipment [11], as shown in Fig. 4. The user equipment (UE) connects to a base station, which directs traffic through a serving gateway (S-GW) over a GPRS Tunneling Protocol (GTP) tunnel. The S-GW serves as a local mobility anchor that enables seamless communication when the user moves from one base station to another. The S-GW forwards traffic to the packet data network gateway (P-GW). The P-GW enforces quality of service policies and monitors traffic to perform billing. The P-GW also connects to the Internet and other cellular data networks, and acts as a firewall that blocks unwanted traffic.

Besides data-plane functionalities, the base stations, serving gateways, and packet gateways also participate in several control-plane protocols. In coordination with the mobility management entity (MME), they perform hop-by-hop signaling to handle session setup, tear-down, and reconfiguration, as well as mobility e.g., location update, paging, and handoff. The S-GW and P-GW are also involved in routing, running protocols such as open shortest path first (OSPF). The Policy Control and Charging Function (PCRF) manages flow-based charging in the P-GW. The Home Subscriber Server (HSS) contains subscription information for each user, such as the quality of service (QoS) profile, any access restrictions for roaming, and the associated MME. In times of cell congestion, a base station reduces the max rate allowed for subscribers according to their profiles, in coordination with the P-GW.

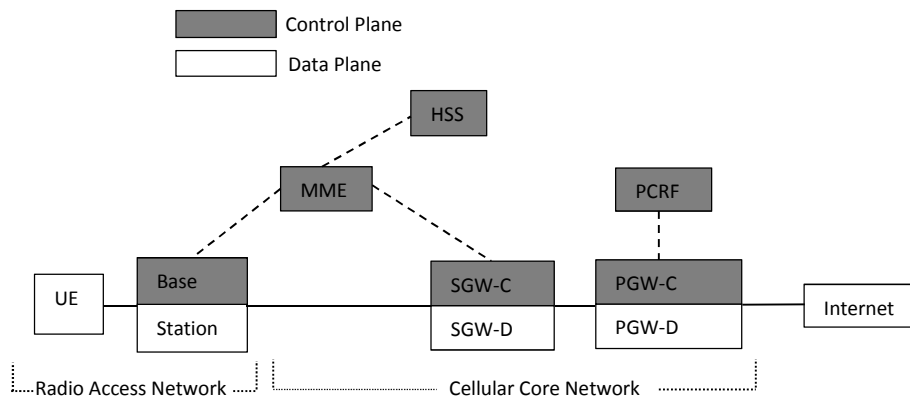


Figure 4. Simplified LTE network architecture

IV. LIMITATIONS OF TODAY'S CELLULAR NETWORK

Today's cellular network architectures have several major limitations. Centralizing monitoring, access control, and quality-of-service functionality at the packet gateway introduces scalability challenges. This makes the equipment very expensive (e.g., more than 6 million dollars for a Cisco packet gateway). Centralizing data plane functions at the cellular-Internet boundary forces all traffic through the P-GW, including traffic between users on the same cellular network, making it difficult to host popular content inside the cellular network. In addition, the network equipment has vendor-specific configuration interfaces, and communicates through complex control-plane protocols, with a large and growing number of tunable parameters (e.g., several thousand parameters for base

stations). As such, carriers have (at best) indirect control over the operation of their networks, with little ability to create innovative services.

V. SDN OVERVIEW

Software Defined Networking is a new architecture that has been designed to enable more agile and cost-effective networks. The Open Networking Foundation (ONF) is taking the lead in SDN standardization, and has defined an SDN architecture model [12] as depicted in Fig. 5.

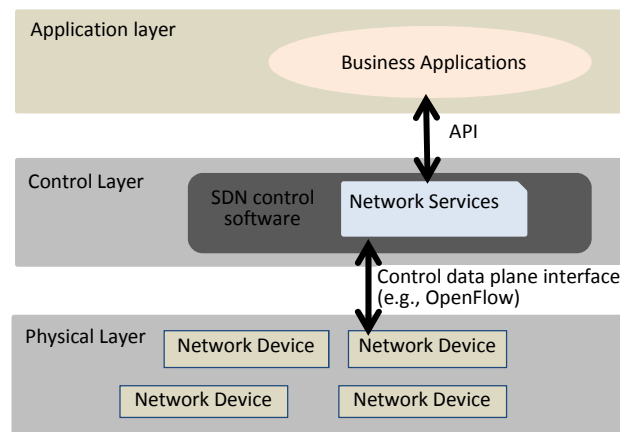


Figure 5. ONF SDN reference model

The ONF/SDN architecture consists of three distinct layers that are accessible through open application programming interfaces (APIs):

- The application layer consists of the end-user business applications that provide different communications services. Communications between the application layer and the control layer is managed by the API.
- The control layer controls and supervises the network forwarding functionality through an open interface.
- The physical layer consists of the physical network devices (i.e. router, switch, etc.) that provide packet switching and forwarding.

According to this model, SDN architecture is characterized by three key attributes:

a) *Logically centralized intelligence*

An SDN provide global network orchestration from a single point of management using the standard interface OpenFlow [13]. By centralizing network intelligence, decision-making is facilitated based on a global (or domain) view where nodes are unaware of the overall state of the network.

b) *Programmability*

An SDN offer programmatic interfaces that can automate and shape network fabric configuration. SDN networks can achieve revolution and differentiation from traditional network by providing open APIs for applications to communicate with the network.

c) *Abstraction*

In an SDN network, the business applications that consume SDN services are abstracted from the underlying network technologies. Network devices are also abstracted from the SDN Control Layer to ensure portability with any application from any vendor.

VI. FUTURE CELLULAR NETWORK ARCHITECTURE

The architecture of future SDN-based cellular network would be something that will handle and manage the full network from a central location and at the same time will enable new services by supporting many subscribers, frequent mobility, fine-grained measurement and control. The future SDN architecture should address real-time adaptation and scalability challenges that today's cellular network usually fails. The typical architecture of SDN-based cellular network is depicted in the Fig. 6.

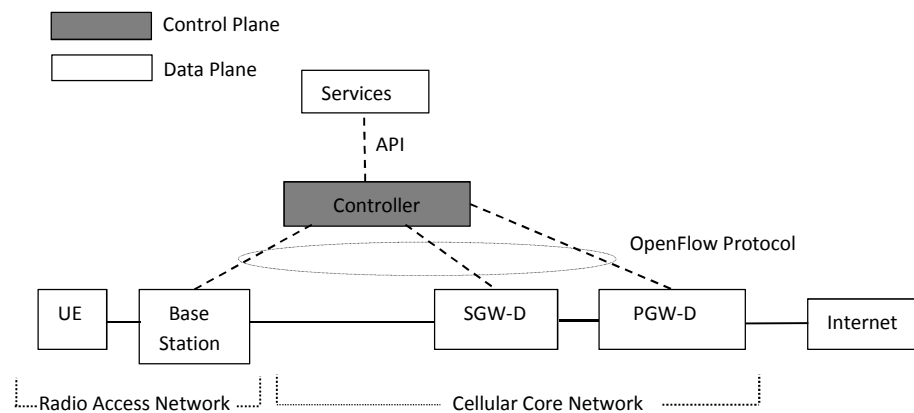


Figure 6. Typical architecture of SDN-based cellular network

From the architectural diagram it is clearly seen that all the controlling functions are separated and instead of a central controller is executed to handle and operate all the network control operations and instruct other components to operate and forward traffic accordingly with the help of different services that reside usually on top of the central controller. The controller communicates with other networking devices by the OpenFlow protocol and maintains the link with the services through open APIs.

VII. RECENT STANDARD PROPOSALS FOR SDN-BASED CELLULAR NETWORK ARCHITECTURE

In this section, a number of proposed SDN-based cellular network architectures have been described that demand to support the challenges of today's and future cellular network.

ONF describes two use cases to illustrate the benefit of OpenFlow (OF) based SDN for mobile networks [14]:

a) Inter-Cell Interference Management

As shown in Fig. 7, the logically centralized control layer enables radio resource allocation decisions to be made with global visibility across many base stations and radio resource management (RRM) decisions can be adjusted based on the dynamic power and subcarrier allocation profile of each base station. In addition, the authors demand that scalability is improved because as new users are added, the required compute capacity at each base station remains low because RRM processing is centralized in the SDN controller.

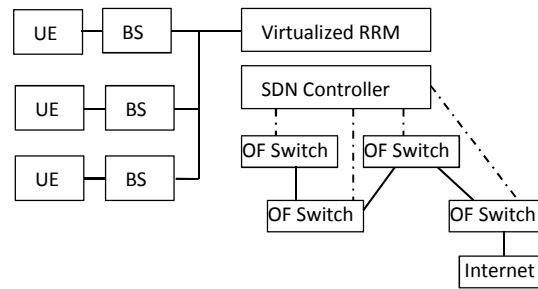


Figure 7. OpenFlow-enabled centralized base station control for interference management

b) Mobile Traffic Management

Offloading or Wi-Fi roaming is a term in communication system that means moving traffic from a mobile network to a Wi-Fi network. The OpenFlow controller (OF controller) will have to interact with entities such as the ANDSF (access network discovery and selection function) for discovering wireless networks close to the mobile user and performing the Wi-Fi offload (Fig. 8). Selection of the roaming destination can be based on a quality of service (QoS) metric such as performance, signal strength, or distance in order to maintain the user experience (UX).

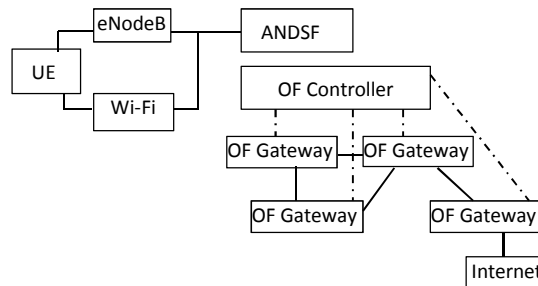


Figure 8. Openflow-based mobile offload

The authors in [11] propose four main extensions to SDN, leading to the architecture in Fig. 9. First, controller applications should be able to express policy in terms of subscriber attributes, rather than IP addresses or physical locations, as captured in a subscriber information base. Second, to improve scalability, each switch should run a local cell agent that performs simple actions (such as polling traffic counters and comparing against a threshold), at the behest of the controller. Third, switches should support more flexible packet classification based on deep packet inspection, and additional actions such as header compression. Fourth, they enable semantic space slicing of the

network resources (a slice in the semantic space is the set of packets whose subscriber attributes satisfy the same predicates). They also enable flexible slicing of base station resources by taking the control out of base stations.

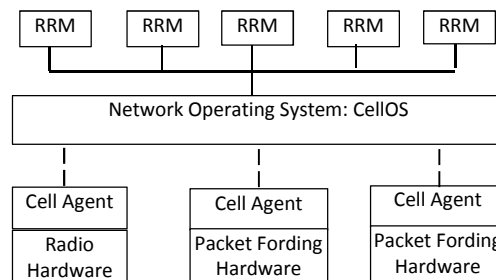


Figure 9. Cellular SDN architecture

SoftCell [15] is an SDN-based cellular network architectural model that demands to support a number of fine-grained services in a scalable manner for cellular core networks (Fig. 10). In this article, the authors used local agents and access switch to each base station to communicate with the controller, they also used OpenFlow switches in the core network rather than EPC/LTE switches. SoftCell interconnects unmodified UEs (via base stations) and the Internet (via gateway switches) and does not require specialized network elements (e.g., S-GWs and P-GWs) or point-to-point tunneling (e.g., user-level GTP tunnels) used in today's LTE networks. SoftCell core network components are as follows:

- a. *Controller*: The controller implements high-level service policies by installing switch-level rules that direct traffic through middleboxes. Service policies are specified on subscriber attributes and application types.
- b. *Access switches*: Each base station has an access switch that performs fine-grained packet classification on traffic from UEs. Access switches can be software switches that run on commodity servers. The server also runs a local agent (LA) that caches packet classifiers for attached UEs, to minimize interaction with the central controller.
- c. *Core switches*: The rest of the network consists of core switches, including a few gateway switches connected to the Internet. These core switches are OpenFlow enabled commodity hardware switches (OFS). They forward traffic through appropriate middleboxes. SoftCell gateway switches are much cheaper than P-GWs; they just perform packet forwarding, and relegate sophisticated packet processing to middleboxes.
- d. *Middleboxes*: SoftCell supports commodity middleboxes such as dedicated appliances, virtual machines, or packet processing rules on switches. Each middlebox function (e.g., firewall) may be available at multiple locations. SoftCell supports stateful middleboxes that require all packets in both directions of a connection to traverse the same instance.

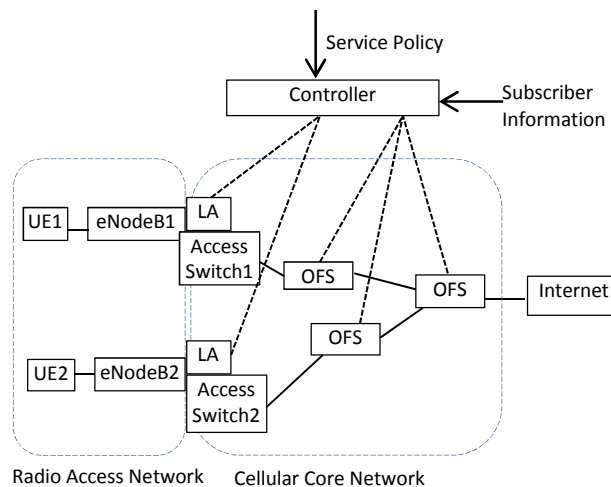


Figure 10. SoftCell Architecture

In a dense wireless deployment with mobile nodes and limited spectrum, it becomes a difficult task to allocate radio resources, implement handovers, manage interference, balance load between cells, etc. In SoftRAN [16], the authors argue that LTE's current distributed control plane is suboptimal in achieving the above objective. They propose SoftRAN, a fundamental rethink of the radio access layer. SoftRAN is the software defined centralized control plane for radio access networks that abstracts all base stations in a local geographical area as a virtual big-base station comprised of a central controller and radio elements (individual physical base stations) as depicted in Fig. 11.

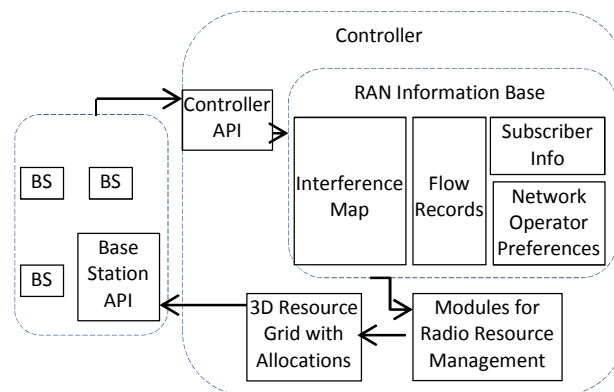


Figure 11. SoftRAN Architecture

SoftRAN achieves the big base station abstraction architecturally as shown in Fig.11. Realizing such architecture has two main challenges:

- Designing a controller which can provide a framework for different control algorithms to operate on.

- Ensuring that the delay between the controller and the radio element does not negatively impact performance.

a) Controller architecture

As shown in Fig. 11, a centralized controller is deployed, which receives periodic updates of local network state from all the radio elements in a local geographical area. Given these updates, the controller updates and maintains the global network state in the form of a database, which we call the RAN Information Base (RIB) that conceptually consists of the following elements:

- *Interference map*: A weighted graph, where each node represents a radio element or an active client in a geographical area and the weight of the edges represent the channel strength between the two nodes.
- *Flow records*: A record of the relevant parameters of an ongoing flow, e.g. number of bytes transmitted, average transmission rate, number of packets queued, etc.
- *Network operator preferences*: In case, the network operator needs to prioritize certain flows over others, he/she can enter his/her preferences into the RIB.

b) Refactoring the control plane

The inherent delay between the controller and the radio elements implies that the radio element has a more updated view of the local state. Thus, in spite of the coordination that a centralized controller provides, the control decisions which depend on rapidly varying network parameters can only be optimized at the radio element. Hence, there is a need to refactor the control functionality between the centralized controller and the radio elements.

There are two main principles guiding the refactoring of the control plane:

- All control decisions that influence the decision making at neighboring radio elements must be made at the controller, since such decisions need to be coordinated across radio elements.
- All decisions that are based on frequently varying parameters should preferably be made at the radio element, since the inherent delay between the radio element and the controller increases the response time to these frequently varying parameters.

In this article [17], the authors propose an SDN-based mobile networking approach integrated with legacy mobility control plane. They simply call this the partially-separated mobile SDN architecture that is compared to the fully-separated mobile SDN architecture where all the control is dominated by a SDN controller without taking the legacy mobility control plane into consideration (Fig. 12). To summarize, they make the following contributions:

- Design SDN-based mobile networking models based on partially-separated control plane with a single control and hierarchical control structures.
- Present the expected applicability for advanced features, which could be expected by the use of the legacy mobility control plane harmonized with SDN.

- Describe the realization of the proposed architectures and implementation challenges and discuss practical deployment issues with current cellular networks.

In the proposed model, the authors demand the advantages of SDN approaches will remain, while the approach will enhance its mobility management capabilities with legacy features used in traditional cellular networks.

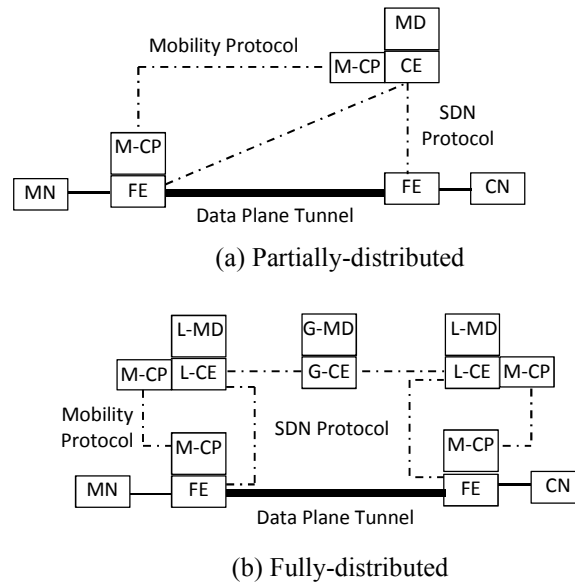


Figure 12. SDN-based mobility management architecture

Specifically, considering different degrees of scalability, they present two different controller structures in the model: single controller and hierarchical controller models. Here they use the term MN for mobile node and CN for correspondent node.

a) *Single controller model*

Fig. 12 (a) represents the proposed single controller model, which gives simplicity without interaction with other controllers. This is adequate for small-scale network deployments such as a campus and small-business enterprise. A mobility anchor point can be determined by the CE, based on routing optimality and monitored network load conditions on FEs. Furthermore, link failure over FEs can be quickly detected and immediately reported to the controller, and thus an alternative route can be established.

b) *Hierarchical controller model*

Fig. 12 (b) shows a more advanced approach, a hierarchical controller model, where the Local CE (L-CE) and Global CE (G-CE) are distinguished for scalability, over the partially-separated SDN architecture. The localized domain enables the controller to swiftly collect network events and enforce relevant commands from/to FEs. Besides, in such a network environment where heterogeneous mobility control mechanisms may be applied, the hierarchical controller model could be effective to control and manage different localized mobility domains as well as to highly improve scalability.

In the article [18], the authors present a new dynamic tunnel switching technique for SDN-based cellular core networks. This approach is to maximally utilize cloud and implement a virtualized EPC (Evolved Packet Core) serving and packet data network gateway (S/P-GW) where control and user plane functions are separated from each other. They demand it would support 5G cellular network. Dedicated packet processing hardware together with dynamic GTP tunnel termination point switching between the cloud and fast path is used to provide user plane processing resources on-demand for each user equipment (UE). The system model and its building blocks are presented in Fig. 13.

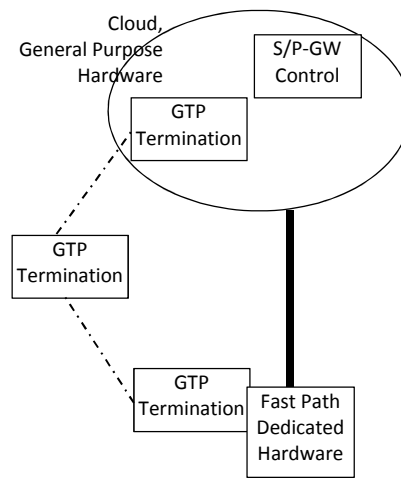


Figure 13. SDN-based virtualized S/P-GW

Both individual UEs and mobile network operators can exploit the new type of dynamicity added to the gateway. The authors demand that they can identify several use cases:

- *Machine-to-Machine (M2M) type of sessions*: Huge amount of low bandwidth sessions are terminated in the cloud but an individual session can be temporarily switched to the fast path for example when motion detection starts video streaming.
- *Optimal routing and offloading capability*: Switching the user plane from the cloud to the fast path located close to the radio network provides optimal routing for the end user and offloading capability to the operator.
- *Overload control*: Dynamic GTP termination can be used to switch a set of sessions to the cloud in order to avoid overloading the fast path element.

A new architecture for SDN-based cellular network (as depicted in Fig. 14) that would be depended on a number of cluster-based controllers rather than a single controller has been proposed in [19]. As cellular data traffic has exploded in recent years and the rate will also be kept in the coming future, the author argued that it would not be possible for a single controller to handle all the functionalities to manage the network.

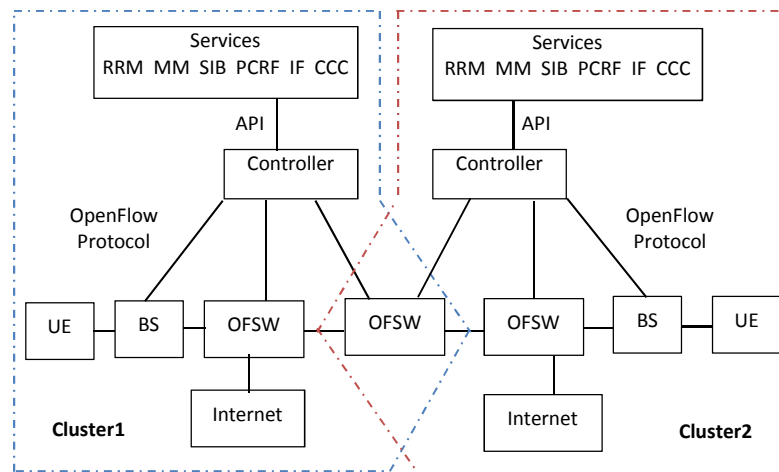


Figure 14. Cluster based Cellular SDN Architecture

To support the services of today's emerging cellular network and at the same time for future network, the author changes the control protocols on the interfaces of S1 (between MME and eNodeB), S11 (between MME and SGW) and S5 (between SGW-C and PGW-C) of the LTE/EPC architecture by the OpenFlow protocol. The other two interfaces S1 (from eNodeB to SGW-D) and S5 (from SGW-D to PGW-D) are controlled by the existing 3GPP protocol of the LTE/EPC architecture. The central controller is responsible to manage all the controlling functions through its different services i.e., RRM, MM, SIB, infrastructure routing (IF), PCRF and controller-controller communication (CCC), that run on top of the OpenFlow controller. The CCC module is the main part of controlling the clusters of the proposed architecture. OpenFlow switches (OFSW) are commodity hardware switches that act like a SGW data plane (SGW-D) and are able to encapsulate/decapsulate GTP packets. This switch applies the rules received from the OpenFlow controller. It is responsible for packet forwarding between the eNodeB and SGW. The architecture also contains Openflow enabled a few gateway switches connected to the Internet. The proposed architecture needs not any change to the radio hardware at the base station; also it does not want extra support to connect to the Internet.

All the above proposals for SDN-based cellular network architectures are in the experimental stages, but have not implemented for the commercial purposes yet. As cellular data traffic has exploded in recent years and the rate will also be kept reasonable in the coming future, cellular networks need an SDN architectural mechanism that will provide fine-grain, real-time control without losing scalability.

VIII. IMPLEMENTATION CHALLENGES OF FUTURE SDN-BASED CELLULAR NETWORK

In order to get the benefits of the SDN-based cellular network the following challenges must be kept in mind and different policies should be made before large scale of real world implementation of future cellular network.

- SGW controller functions must be separated from the data plane functions and should be included in the central controller as separate applications. This is not an easy work for the existing cellular network as all the

nodes should be changed to SDN-enabled devices to get the full benefit of SDN network. However, there is good news for network operators that recently SDN specific application specific standard products (ASSPs) have been introduced by Intel, Broadcom and Marvell targeting primarily high performance Ethernet switching with virtualization and OpenFlow support for over 500 Gbps switching. Also, other system vendors (e.g. Cisco, Huawei, Juniper etc.) are expected to make SDN products that would be comprised of proprietary application specific integrated circuits (ASICs) to implement the SDN data plane.

- The OpenFlow controller should have a global network view and the ability to control and manage all the forwarding units in the network. At the same time, it must be able to communicate with all the base stations to update the traffic information so that same controlling information could be available both at the base stations and the central controller. In this case, it would be difficult for a single controller to communicate to all the nodes simultaneously with the same speed as there may be some latency introduced by exchanging network information between multiple nodes and a single controller. A distributed or peer-to-peer controller infrastructure would minimize the load by sharing the communication messages of the controller. Nevertheless, this method would also increase the overhead of controller-to-controller interactions raising the traffic loads.

- The controller should be able to identify the attachment and detachment of the end user equipment during the handover procedure. This would not be very difficult for a single central controller based cellular network as it is generally easy to view the whole network from that controller. However, if there would be more than one controller and the handover will be occurred to an end device that will go from one controller to another how they will communicate with one another to handle the soft handoff and whether a single controller or both will be really responsible to process the whole job.

- The controller is needed to handle a large database to store the required information of networking states of every second for smooth communication between the end users. A large memory, IO devices, CPU capabilities should be required to handle and calculate each session for routing, mobility management and QoS activities. To overcome the problem of the size and operation of the controller back-end database, one solution would be a way where a volume of queries can be processed in the node CPU, which would otherwise be transferred to the central controller for processing. This will possibly decrease the database size at the controller and concurrently minimize communication between the controller and its nodes.

- The MME, HSS, PCRF functions should be imposed as separate applications on top of the central controller for exchanges transparently. With these services other application or services would be served by the controller as the time goes on. For example, security issues would be a great challenge for SDN based cellular network. The controllers will be particularly attractive target for attack in the SDN architecture open to illegal access and misuse. Also, in the lack of a strong, secure controller platform, it will be possible for an attacker to act as a controller and carry out malicious activities.

- Finally, to deploy SDN-based cellular network in an existing cellular network, it is really essential to handle and manage both GTP and OpenFlow protocols at the same time in the same network. This is the most crucial challenges of implementing SDN concept in an existing cellular network. It would be honestly easy to

install a completely new infrastructure for cellular network based on SDN technology. For this, all elements and devices in the network would be SDN-enabled and OpenFlow supported. Conversely, there exists a vast, installed-base of cellular networks supporting vital systems, organizations and businesses today. To simply convert these networks for new infrastructure would not be easy and will be only well suited for closed environments, such as data centres and campus networks.

IX. CONCLUSION

Despite the extraordinary success of the cellular mobile telecommunications industry, many of the underlying design strategies and service assumptions that have served us arguably well over the past few decades may benefit from a fresh new look. Indeed, the LTE network architecture called Evolved Packet Core (EPC), does eliminate a few network elements, and simplifies some of the RAN architecture. Although, it was a change in the right direction, the result appears to provide somewhat constrained enhancements in terms of reduction in complexity and improvement in flexibility.

The future of the mobile cellular network is difficult to envision with specifics beyond a few general observations: There will be far more devices, orders of magnitude more base stations connecting them, and numerous different applications - ever changing - running over the network. In this article, various architectural aspects and features of today's and future SDN-based cellular network has been performed, and at the same time a number of implementation challenges are focused that should be kept in mind before getting the benefits of the SDN-based cellular network; an incrementally deployed SDN-based architecture will be designed for today's existing cellular network for future work.

ACKNOWLEDGEMENT

The author thanks to his family members and the researchers whose research papers are included in this article.

REFERENCES

- [1] IBM Systems and Technology, "Software Defined Networking - A new paradigm for virtual, dynamic, flexible networking", October 2012
- [2] Kirk Bloede, "Software Defined Networking – Moving Towards Mainstream", Electronics Banking Research, August 2012
- [3] Brocade VCS Fabrics: The Foundation for Software-Defined Networks
- [4] "Network Transformation with Software-Defined Networking and Ethernet Fabrics", Brocade Communications Systems, Inc., 2012
- [5] Md. Humayun Kabir, "Software Defined Networking (SDN): A Revolution in Computer Network", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 15, issue 5 (Nov. - Dec. 2013), pp. 103-106
- [6] "Software Defined Networking: What Is It and Why Do You Need It?", enterasys secure network
- [7] <http://globalconfig.net/software-defined-networking-vs-traditional/>
- [8] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks"
- [9] <http://www.brocade.com/solutions-technology/technology/software-defined-networking/openflow.page>
- [10] David Tipper, Prashant Krishnamurthy, and James Joshi, "Network architecture and protocols for mobile positioning in cellular wireless systems", Department of Information Science and Telecommunications, University of Pittsburgh, Pittsburgh, PA 15260.
- [11] Li, L. E., Mao Z. M., Rexford J. "Toward Software-Defined Cellular Networks", In Proceedings of IEEE EWSN. 2012.
- [12] "ONF", <https://www.opennetworking.org/>

- [13] "OpenFlow Switch Specification", version 1.3.2. Open Networking Foundation. 2013.
- [14] "OpenFlow™-Enabled Mobile and Wireless Networks", ONF Solution Brief, September 30, 2013.
- [15] Jin X., Li L. E., Vanbever L., Rexford J. SoftCell: Scalable and Flexible Cellular Core Network Architecture. In Proceedings of ACM CoNEXT. 2013.
- [16] Aditya Gudipati, Daniel Perry, Li Erran Li, Sachin Katti, "SoftRAN: Software Defined Radio Access Network", HotSDN'13, August 16, 2013, Hong Kong, China.
- [17] Seil Jeon, Carlos Guimarães, Rui L. Aguiar, "SDN-Based Mobile Networking for Cellular Operators", MobiArch'14, September 11, 2014, Maui, Hawaii, USA.
- [18] Johanna Heinonen, Tapio Partti, Marko Kallio, Kari Lappalainen, Hannu Flinck, Jarmo Hillo, "Dynamic Tunnel Switching for SDN-Based Cellular Core Networks", AllThingsCellular'14, August 22, 2014, Chicago, IL, USA.
- [19] Md. Humayun Kabir, "A Novel Architecture for SDN-based Cellular Network", International Journal of Wireless and Mobile Network (IJWMN), vol. 6, no. 6, December 2014.

Realization of information exchange with Fibo-Q based Symmetric Cryptosystem

Shaligram Prajapat
Computer Applications Department MANIT
MANIT Bhopal

Ramjeevan Singh Thakur
Computer Applications Department MANIT
Bhopal (MP), India

Abstract—Secured information exchange is demand of e-world. Numerous techniques are being evolved and experiment to share large files. Symmetric cryptosystem based algorithm works in this direction. In this paper we have discussed result of implementation of our proposed algorithm [11] based on Fibo-Q matrix. This algorithm employs generation using automatic variability concept. The corresponding numerical analysis and effective gain has also been noticed. This approach will not only enhance the security of information but also saves computation time and reduces power requirements that will find it's suitability for future hand held devices and online transaction processing.

Keywords—cipher; key; Enciphering; Decipherment; fibonacci; Q- matrix; symmetric key algorithm, automatic variable key.

I. INTRODUCTION

“Security of a crypto system must be totally dependent on the secrecy of the key, not on the secrecy of algorithm” this statement of Sir Kerchoff given in 1883 is still relevant in current modern era [1]. It is also important to know keeping the algorithm secret; it would be very difficult to keep the inner working of a cryptosystem secret. Underlying algorithm can be discovered by reverse-engineering. It is safer to follow kerchoff's principle and release the crypto-system for public reviews. Hence for a successful cryptosystem secrecy of key is important. In recent era exchange of all the information including financial and e-commerce transaction takes place among parties or entities that might not known to each other but participates in communication. During this transmission of information public network is used hence ensuring the security of these information and confidentialities of involved parties is mandatory. The information stored in computers or during information, to avoid unauthorized access or damage of information technique known as Encryption and Decryption mechanism is used. Before transmission of information Encryption and after receiving of information Decryption process is used. Securing information based on used key is classified into symmetric, asymmetric or hash. If both sender and receiver use the same key then it is symmetric cryptosystem. And if encryption and decryption key are different then it is known as asymmetric cryptosystem. In any of the situation, the used key decides the level of security of cryptosystem. There are various alternatives to control the security of a cryptosystem like Hind the Encryption, Decryption algorithms. But by doing reverse engineering if the behavior of algorithm is known then whole cryptosystem will fame. Or by increasing the key size (Increasing the key size will result in increase in key guess time or by increasing brute force attack time/trials that ultimately will increase the system security. But increasing the key size will increase the time in encryption or decryption process .By increasing computing resources or energy required to process will definitely be affected once the key length has been increased beyond a threshold. Hacker or cryptanalyst may use parallel processing; multiword computing and advanced algorithms usage may lead to compromise the system security.

Another alternative in this direction we fixed up the key with a specific length and try to vary it from session to session. This approach forms the basis of self variable key based AVK-Model, In this AVK model as we fixed up the length of key to a minimum threshold then the number of resources are freed. Up. Since the key varies from session to session so if hacker or cryptanalysis gains the access of key of a particular session even though it is invalid for next session. So the level of security of cryptosystem is enhanced. In AVK model. since the key changes from session to session, so the issue of new key exchange arises .To handle this issue we apply parameters AVK model that exchanges only parameters for key generation. Since on the public network only parameters are exchanged, so both sender and receiver will computer key at their own end and construct the key.

The AVK approach with parameterized model is to be investigated from the perspective of hackers or cryptanalyst. The detailed analysis will decide the success of the AVK model of symmetric cryptosystem. This analysis is termed as Cryptic Mining. Cryptic mining is a set of cryptic algorithm that analyses the captured plaintext-cipher text, plaintext-key logs, parameters-key logs and captured cipher logs and provides useful knowledge, process and developing the knowledge based or AI based framework. In future cryptic mining algorithm group will be useful for auditing and classification of cryptic algorithms. Theoretically cryptic algorithms provides random ciphers, but in practice it is not so, these algorithm uses pseudo random numbers that are generated by some computer or mathematical formula. So these ciphers have some sort of patterns, by extracting these patterns cryptic mining algorithms may find possible sequence or hints about key or association among key and plaintext or cipher. Depending upon the degree of patterns in the output the class of cryptic algorithms can be decided. In this way, in future AVK algorithm may contribute in the extension of symmetric algorithm design. Certainly this provide strength to mechanism of maintenance and exchange of information.

Cryptographic algorithms are classified in two general types: Symmetric and Asymmetric algorithms. In *Symmetric algorithms* Enciphering key can be calculated from the Decipherment key and vice versa. In most symmetric algorithms, the Enciphering and Decipherment key are the same. Both the sender and receiver agree on a key before they can communicate securely. On the other hand, in *Asymmetric algorithms* the Decipherment key cannot be calculated from the Enciphering key. So, keys play an important role in the security of any cryptographic algorithm. If weak key is used in algorithm, then any intruder may decrypt the data. One of the central factors contributing to the strength of symmetric key algorithms is the size of key used. In practice, most state-of-art cryptographic algorithms rely on increasing the key size to strengthen the security of algorithm [2]. In this paper, we instead focus for power efficient and fast algorithm based on varying the key to increase the security of algorithm.

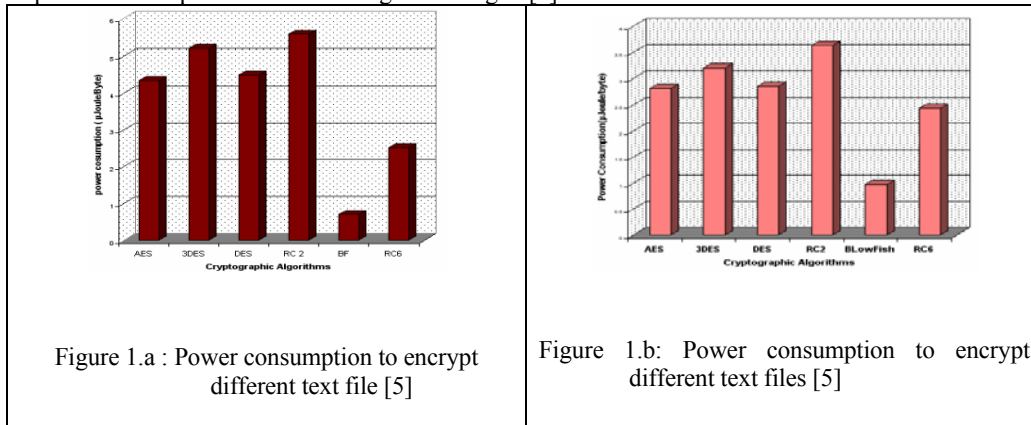
II. RELATED WORK

Symmetric algorithms can be Block ciphers or Stream ciphers. *Block cipher* processes the input one block of element at a time, producing an output block for each input block. *Stream ciphers* process the input element continuously, producing output one element at a time, as it goes along. In [1, 2, 3, 6], various cryptographic algorithms and their applications have been defined and discussed. Following table 1 summarizes some block cipher algorithms. Asymmetric algorithms are almost 1000 times slower than symmetric algorithms, because they require more computational processing power [4].

Table 1: Summary of some symmetric block cipher algorithms

S. No.	Algorithm	Block size	Key length
1	DES	64 bits	56 bits
2	3DES	64 bits	168, 112 or 56 bits
3	RC2	64 bits	8-128 bits (variable length key)
4	Blowfish	64 bits	32-448 bits (variable length key)
5	AES	128 bits	128, 192 or 256 bits
6	RC6	128 bits	128, 192 or 256 bits
7	RSA	-	1024-2048 bits (variable key length)

A study was performed for analyzing the performance of security algorithms by varying the key size. The effect of changing the key size on power consumption in shown in Fig. 2 and Fig. 3 [5].



The result of varying the key size of AES (symmetric algorithm) on computation time in shown in Fig. 4.

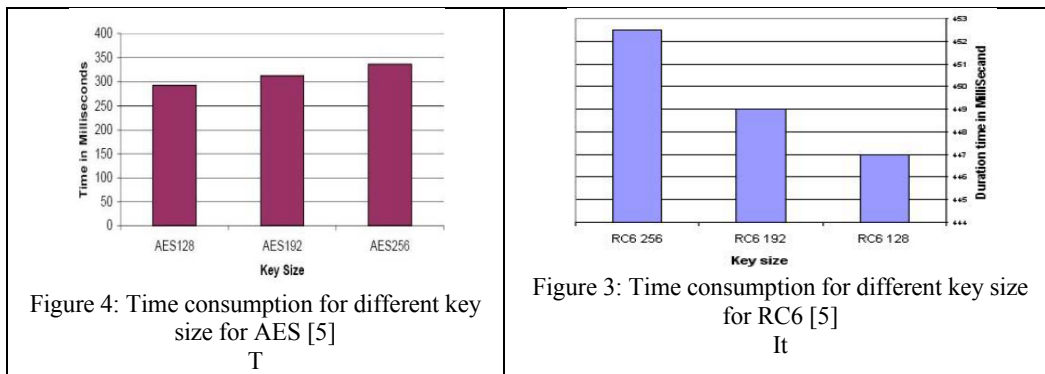


Figure 3: Time consumption for different key size for RC6 [5]
It

The result of varying the key size of RC6 (symmetric algorithm) on computation time in shown in Fig. 5. It is clear that larger key sizes lead to increase in computation time and battery power consumption. The reversible functions are necessity of symmetric key algorithms. Many well known symmetric algorithm have been proposed using reversible XOR function. Stakhov [8] proposed a coding/decoding system based on Fibonacci Q-matrix. The Q-matrix is based on following concepts:

A. Fibonacci-Number

The Fibonacci numbers are obtained by following recursive function

$$\begin{aligned} F_n &= n & \text{if } n = 0 \text{ or } n = 1 \\ F_n &= F_{n-1} + F_{n-2} & \text{if } n > 1 \end{aligned}$$

B. Fibonacci Q-Matrix

$$Q = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Where $\text{Det}(Q) = -1$.

The nth power of this Q-Matrix can be computed as follows:

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \text{ Where } F_{n-1}, F_n \text{ and } F_{n+1} \text{ are Fibonacci numbers.}$$

Since $\text{Det}(A^n) = (\text{Det } A)^n$

Therefore, $\text{Det}(A^n) = (-1)^n$ where $n \in \mathbb{N}$

Following identity connects three neighboring Fibonacci numbers: $F_{n-1} + F_n + F_{n+1} = (-1)^n$

Also, $Q^n = Q^{n-1} + Q^{n-2}$

$\Rightarrow Q^{n-2} = Q^n - Q^{n-1}$

Where:

$$Q^{-n} = \begin{pmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{pmatrix}$$

Algorithm-1 iFibonacci (index n)	Algorithm-2 rFibonacci (index n)
<pre> { if (n<= 1) then output(n); else { ft2 ← 0; ft1 ← 1; for I ← 2 to n in steps of 1 do { ft ← -ft1+ft2; ft2 ← ft1; ft1 ← ft } Output(ft) } </pre>	<pre> { if (n<= 1) return n; else return(rFibonacci (n-1)+rFibonacci (n-2)); } </pre>



Fig.4 iterative and recursive variants for computing individual elements of fibo-QAlgorithm

C. Fibonacci Enciphering/Decipherment algorithm:

Fibonacci Q-matrices allow us to develop a symmetric algorithm. This algorithm assumes an initial message in the form of square matrix M of size $(p+1) \times (p+1)$ where $p = 0, 1, 2, 3 \dots$. Now choose the Fibonacci Q_p -matrix, Q_p^n , of size $(p+1) \times (p+1)$ as a Enciphering (key) matrix and it's inverse matrix, Q_p^{-n} , of the same size as Decipherment (key) matrix. Therefore, the Enciphering and Decipherment are defined by parameters n and p .

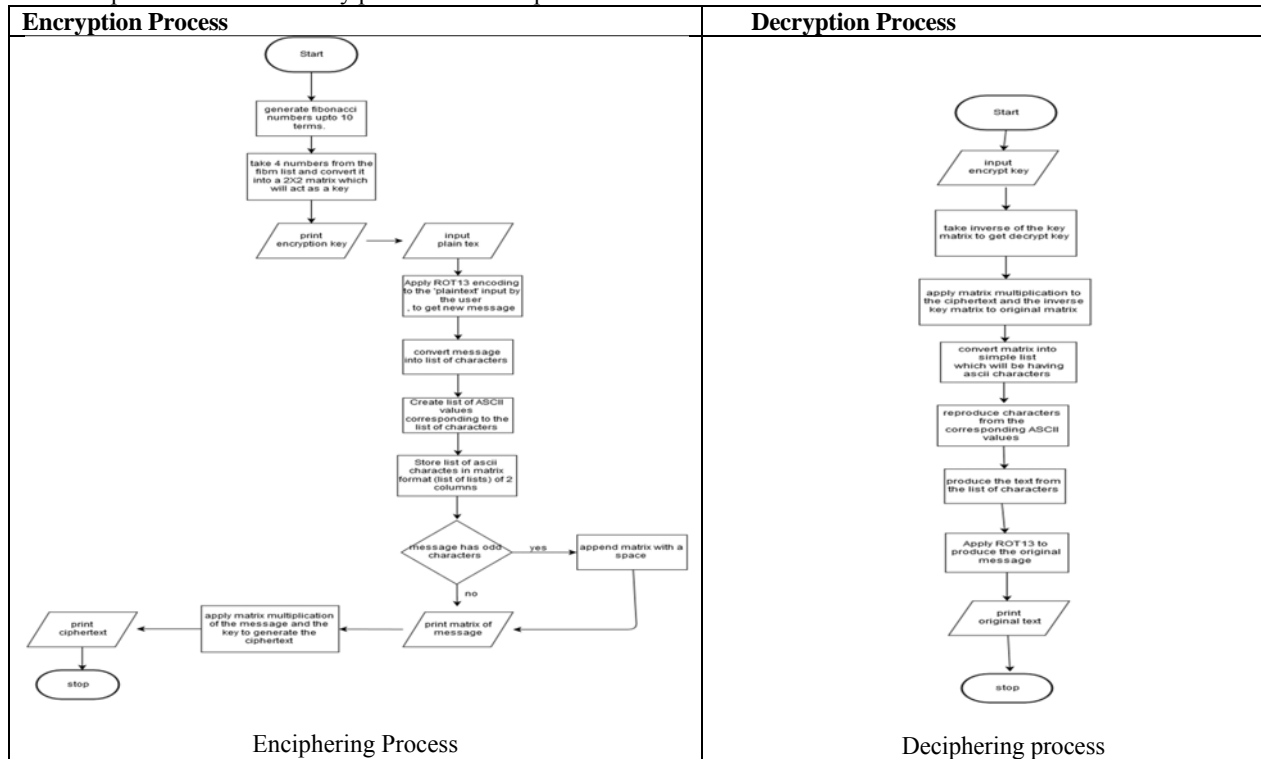


Fig. 4. Fibo-Q based Enciphering and Deciphering Process

The working of above symmetric key Enciphering algorithm based on classical Q-matrix is beautifully illustrated in [8] and [9].

<i>Fibo_Enciphering algorithm:</i>	<i>Fibo_Decipherment algorithm:</i>
<pre> Algorithm fibo_encrypt (plaintext M) { 1. Choose n. 2. Choose p. 3. Compute Q_p^n. 4. $E \leftarrow M \times Q_p^n$ // Compute Cipher text 5. Return (Cipher _Text E). } </pre>	<pre> Algorithms fibo_decrypt (n, p, E) { 1. Compute Q_p^{-n}. 2. $M \leftarrow E \times Q_p^{-n}$ // Generate Plain text. 3. Return (Plaintext M) } </pre>

A. P. Stakhov et al [8, 9] explained the Decipherment process is shown in fig. 5. Above algorithm has been analyzed, implemented and tested [10] and they concluded that the algorithm works faster than symmetric algorithms (including DES, 3DES, AES and Blowfish). In this paper, the idea of time varying key (using Fibonacci Q-matrix) has been suggested. Very little work has been done in this direction. P. Chakrabarti et al [7] proposed some approaches which are yet to be investigated experimentally.

III. PROPOSED METHOD

This section will exploit automatic variable key technique where the session-key is keeps changing from session to session. Where if Trudy has access of key of some session, then it would not be valid for deciphering of the plain text message in

subsequent sessions. The enhancement of the security algorithm is achieved by using the variability of key computed from Q matrix whose elements are constituted from Fibonacci function. Both the Sender and receiver computes Fibonacci Q-matrix, as a AVK using parameter n and p , to generate cipher text. At transmission end Alice multiplies Q matrix with message block of dimension say of $(p \times 2)$ with key of dimension (2×2) to generate cipher text. As a receiver Bob can then apply inverse operation of this Fibonacci Q-inverse Matrix to decode or regenerate transmitted plaintext-message [8]. This Fibonacci Q matrix acts as a reversible XOR operator. The Q matrix at a particular session with given parameters, n and p values, contains key components F_{n-1} , F_n and F_{n+1} . Thus for one session the sender and receiver not only have the key of current session but also probable keys of previous and next session. Here key (n, p) is made to vary from session to session hence even if the intruder gets unwanted access to the key of session r , it would not be valid for original message extraction in session $(r+1)$ onwards. This enhances the security of algorithm and using the reversibility of Fibonacci Q-Matrix the receiver will receive the data correctly after the application of Q_p^{-n} .

IV. IMPLEMENTATION AND RESULT

The scheme proposed in previous section has been implemented in python and the code snippet of Enciphering and Decipherment was tested for large values of n . The code segments of Enciphering and Decipherment with rot-13 is as follows using

Python implementation is elucidated below.

ENCIPHERING	DECIPHERMENT
<pre> def encrypt(key): plaintext = raw_input("Please enter your plaintext message: ") print "Input plaintext = ", plaintext rot13_text = plaintext.encode("rot13") chars_rot13_text = [] ascii_chars_rot13_text = [] count = 0 for i in rot13_text: chars_rot13_text.append(i) for u in chars_rot13_text: ascii_chars_rot13_text.append(ord(u)) ascii_chars_rot13_text_matrix = [] temp = [] for entry in ascii_chars_rot13_text: if count != 2: temp.append(entry) count = count + 1 if count == 2: ascii_chars_rot13_text_matrix.append(temp) temp = [] count = 0 if len(ascii_chars_rot13_text)%2 != 0: temp.append(32) ascii_chars_rot13_text_matrix.append(temp) ciphertext = matrix_multiplication(ascii_chars_rot13_text_matrix, key) return ciphertext </pre>	<pre> def decrypt(ciphertext, decrypt_key): print "Ciphertext = ", ciphertext resmat = matrix_multiplication(ciphertext,decrypt_key) result = [] for u in resmat: for t in u: result.append(t) result2 = [] for y in result: result2.append(chr(y)) orig_text = ".join(result2) plaintext = orig_text.encode("rot13") return plaintext </pre>

Complexity Analysis

The time complexity of this iterative-Fibonacci for (n>1) is 4n+1.

For recurrence the definition would be as follows:

$$F(0) = 0 \text{ else } F(n) = 2F(n-1) + 1$$

. Applying substitution method for solving this recursive definition.

$$F(n) = 2F(n-1) + 1$$

$$F(n) = 2*(2F(n-2) + 1) + 1$$

$$F(n) = 4*(2F(n-3) + 1) + 1 + 2$$

:

$$F(n) = 2^k * F(n-k) + \sum 2^i$$

$$F(n) = 2^k * F(n-k) + 2^{(k-1)}$$

$$F(n) = 2^k * F(n-k) + 2^k - 1$$

For the base condition, $n-k = 0 \Rightarrow n=k$

$$F(n) = 2^n * F(n-n) + 2^n - 1$$

$$F(n) = 2^n * F(0) + 2^n - 1$$

$$F(n) = 0 + 2^n - 1$$

$$F(n) = 2^n - 1$$

$$F(n) = O(2^n)$$

The graph for various values of Fibonacci number and corresponding computation time is drawn below. It also affirms that for large values of n our will be superior to the traditional algorithms with XOR operations. Higher the values of n take longer the time to compute. Specifically for $n > 3000$. This also makes harder for an intruder to perform cryptanalysis. This assures that our algorithm may be a better alternative as compared to those algorithms that relies on increasing the key size for enhancing the security of a cryptosystem.

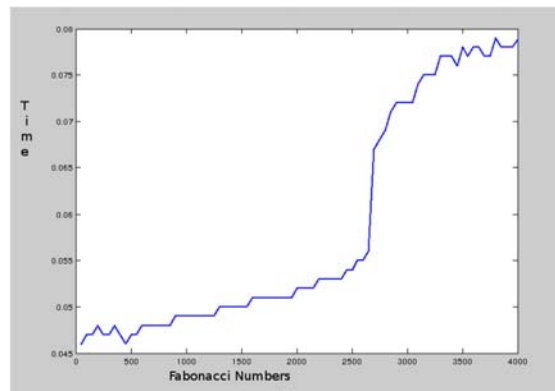


Figure 6: Time Computation for our algorithm to encrypt different text document files

Key size (number of digits)	Fibonacci
1	1.2927041053771973
2	1.3459727764129639,
3	1.5069561004638672
4	1.4363939762115479

Result Table showing execution times for computing different key size (in number of digits.)

V. FUTURE WORK AND SCOPE.

This work provides detailed description of AVK model of symmetric encryption using fibo-Q matrix, with time complexity and implementation. The Fibonacci Q-matrix with Rot-13 Enciphering works fine for large values of input size n . The design is to be tested from hackers' perspective also. Another issue is to use number of digits to be used actually for key exchange. The alternative approach for symmetric key algorithms based on variability of key instead of increasing key size is the major issue. It's vulnerability from intruders point of view may be another direction in this regards.

REFERENCES

- [1] William and Stalling, *Cryptography And Network Security*, 4/E. Pearson Education India, 2006.
- [2] B. Schneier, *Applied cryptography: protocols, algorithms, and source code* in C. Wiley, 1996.
- [3] Maxime Fernández¹, Gloria Diaz¹, Alberto Cosme¹, Irtalis Negrón¹, Priscilla Negrón¹, Alfredo “Cryptography: algorithms and security applications” *The IEEE Computer Society’s Student Fall 2000* Vol. 8 No. 2.
- [4] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, “Performance Evaluation of Symmetric Enciphering Algorithms,” *International Journal of Computer Science and Network Security*, vol. 8, no. 12, pp. 280–286, 2008.
- [5] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, “Performance Evaluation of Symmetric Enciphering Algorithms on Power Consumption for Wireless Devices,” *International Journal of Computer Theory and Engineering*, vol. 1, no. 4, pp. 1793–8201, 2009.
- [6] M. Hellman, “An overview of public key cryptography,” *IEEE Communications Magazine*, vol. 16, no. 6, pp. 24–32, 1978.
- [7] P. Chakrabarti, B. Bhuyan, A. Chowdhuri, and C. Bhunia, “A novel approach towards realizing optimum data transfer and Automatic Variable Key (AVK) in cryptography,” *IJCSNS*, vol. 8, no. 5, p. 241, 2008.
- [8] Stakhov A.P., “Fibonacci matrices, a generalization of the ‘Cassini formula’, and a new coding theory,” *Chaos, Solitons & Fractals*, vol. 30, no. 1, pp. 56–66, Oct. 2006.
- [9] A. NALLI, “On the Hadamard Product of Fibonacci Qn matrix and Fibonacci Q- n matrix,” *Int. J. Contemp. Math. Sciences*, vol. 1, no. 16, pp. 753–761, 2006.
- [10] A. Nadeem and M. Y. Javed, “A performance comparison of data Enciphering algorithms,” in *Information and Communication Technologies*, 2005. *ICICT 2005. First International Conference on*, 2005, pp. 84–89.
- [11] Shaligram Prajapat, Amber Jain and Dr.R.S.Thakur ,” A novel approach for information security with automatic variable key using Fibonacci Q-matrix” *International Journal of Computer & Communication Technology (IJCCT)* ,Volume 3, Issue 3, 2012,pp.54-57

Dynamic Analysis Tool for Detecting SQL Injection

Ahmed Khalid

*Department of computer science
Community College, Najran University
Najran
KSA*

Musab M.F.Yousif

*department of computer science
college of computer science, University of Nileen
Khartoum
Sudan*

Abstract—In this paper the researchers introduce a simple algorithm by using dynamic code analysis tool for the web application to detect SQL injection vulnerability. The function of the proposed tool is depends on the extraction of the suspected GET and POST methods in the web application and checking the possibility of injecting SQL vulnerable statements. The proposed algorithm is tested using popular web sites online. Experiment is conducted to demonstrate the performance of proposed tool.

I-Introduction

Hackers can easily access web application's underlying database by using many techniques [1,26]. SQL injection is one of the most harmful attack techniques used by hackers to vulnerable web applications. SQL injection is one of the most harmful vulnerabilities that can lead to exposure of all the sensitive information stored in an application's database, including handy information such as usernames, passwords, names, addresses, phone numbers, and credit card details[12,18]. SQL injection attacks have been used to extract customer and order information from e-commerce databases, or bypass security mechanisms[5,14]. SQL injection is a technique often used to exploit database systems through vulnerable web applications [21,22]. Nowadays most web applications are being hacked using SQL Injection attacks method, the papers [16,25] classify it as the top ten security threats in the web applications. UK Security Breach Investigations Report classify SQL injection as 40% of web attack in 2010 [21]. This attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. The technique allows the attacker to not only steal the entire contents of relational databases but also, in many cases, to make arbitrary changes to both the database schema and the contents [28, 9, 3, 24].

The treatment of SQL injection problem is provided by the class of attack prevention techniques that retrofit programs to shield themselves against SQL injection [8, 27, 15, 17]

SQL injection attack techniques can be classified into two categories, vulnerability identification approaches and attack prevention approaches [23]. The identification approach based on researching for vulnerable locations in a web application which may lead to SQL injection attacks. Programmer often try to test all inputs by input validation and filtering routines in order to avoid SQL injection attacks [2,3]. Traditional SQL injection attack countermeasures are not active [6,4,20] and most web applications deployed today are still vulnerable to SQL injection attacks.

SQL injection attacks detection and prevention include applications using black or white list input filters, using special APIs, static analysis detection tools or detecting SQL injection attacks at runtime [30]. The technique presented in [13, 29] represent the static analysis techniques for vulnerability identification and the approaches introduced in [7,19] represent the detection of SQL injection attacks at runtime. Paper [13] presents some ways to avoid SQL injection attacks, which are:

1. Minimum use of dynamic SQL queries should be made if there is some alternative way.

2. The Stored procedure must be executed using a safe interface such as callable statements in JDBC or command object in ADO
3. All the input from the user must be validated thoroughly.
4. In order to run the database, the use of low privilege account must be made.
5. Proper roles & privileges must be given to the stored procedure that is used in the application.
6. Use of parameterized stored procedures with embedded parameters must be made.

In HTML, a form is used to pass the data from a web browser to a web server. For example, if logging into a web page, you will input your username and password inside registration form. Then, by clicking the "sign in" button you're submitting your username and password from your web browser to the webserver [10]. Two different submission methods for a form can be used with its attributes, these are the GET and POST methods [11]. These two methods can be hacked by using SQL injection attacks. This paper introduces a tool to detect SQL injection attacks at runtime. The proposed tool is tested against a list of webpages to check the existing of SQL injection vulnerability.

The rest of this paper is organized as follows: in Section II the structure of the SQL injection detection tool is introduced. Section III shows the results and discussion. The paper concludes by section V.

II- The SQL Injection Detection Tool

The proposed SQL Injection Detection tool is based on the HTTP request send by clients or users and look for attack signatures. The tool is composed of two stages:

1. Collecting the information from the web pages which is done by three steps extracting the URL addresses, collecting the parameters value passed by GET method, and collecting the parameters value passed by POST method.
2. Detecting SQL injection vulnerability by injecting the collected POST and GET methods vulnerable SQL statements.

Stage 1:

- 1- Extracting the URL addresses is done by looking for "href=" in the HTML code. The tool collect URL for three level of web pages (the first page as the first level, the pages belong to the links in the first page as the second level and the pages reached by the links in the second level as the third level) Fig1 shows the flowchart for this stage. The collected URLs is sorted and the duplication is removed.

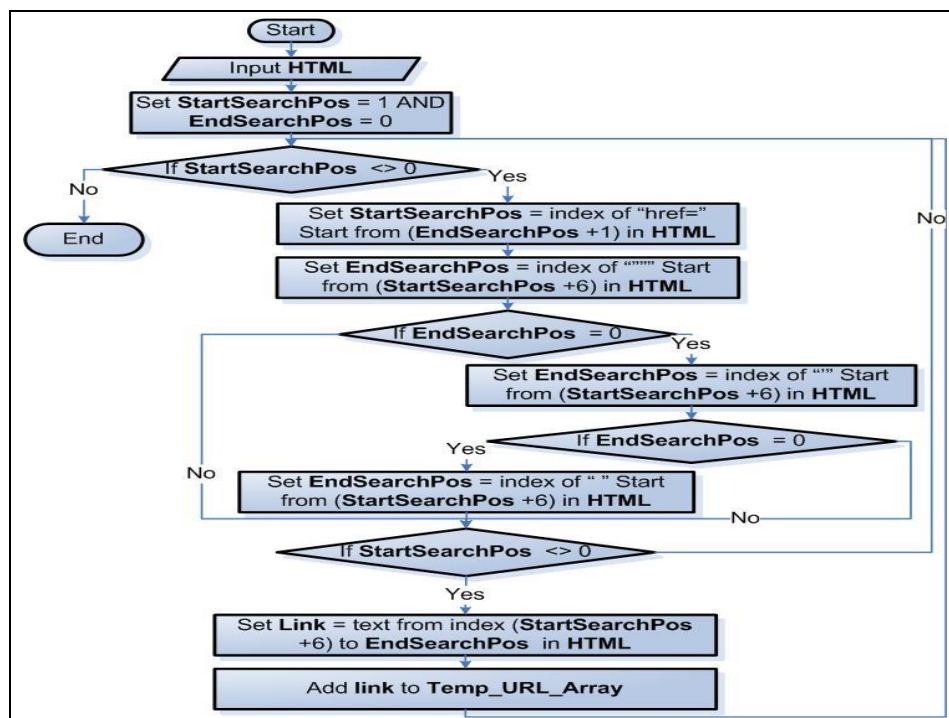


Fig 1: URL extraction flowchart

- 2- Collecting the parameter values passed by GET method is done by extracting the GET parameters in any of the links included in the web pages . Fig2 show the flowchart of this step

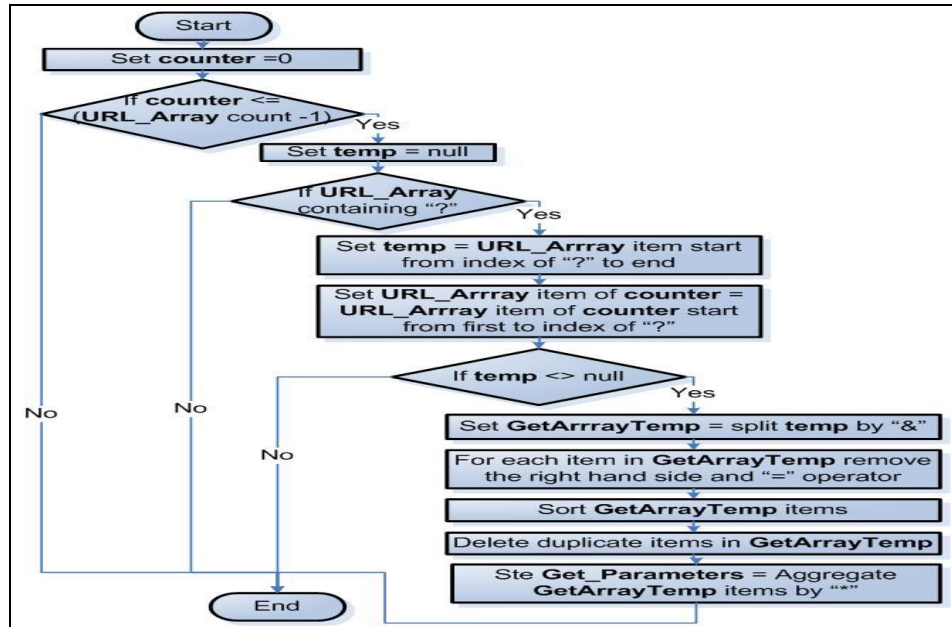


Fig2: Collection of the GET method parameters

- 3- Collecting the values passed by POST method is done by analyzing the HTML code searching for “input” tag. The tags that bear type “text” or “pass” or “hidden” are selected. Fig3 shows the flowchart for this step.

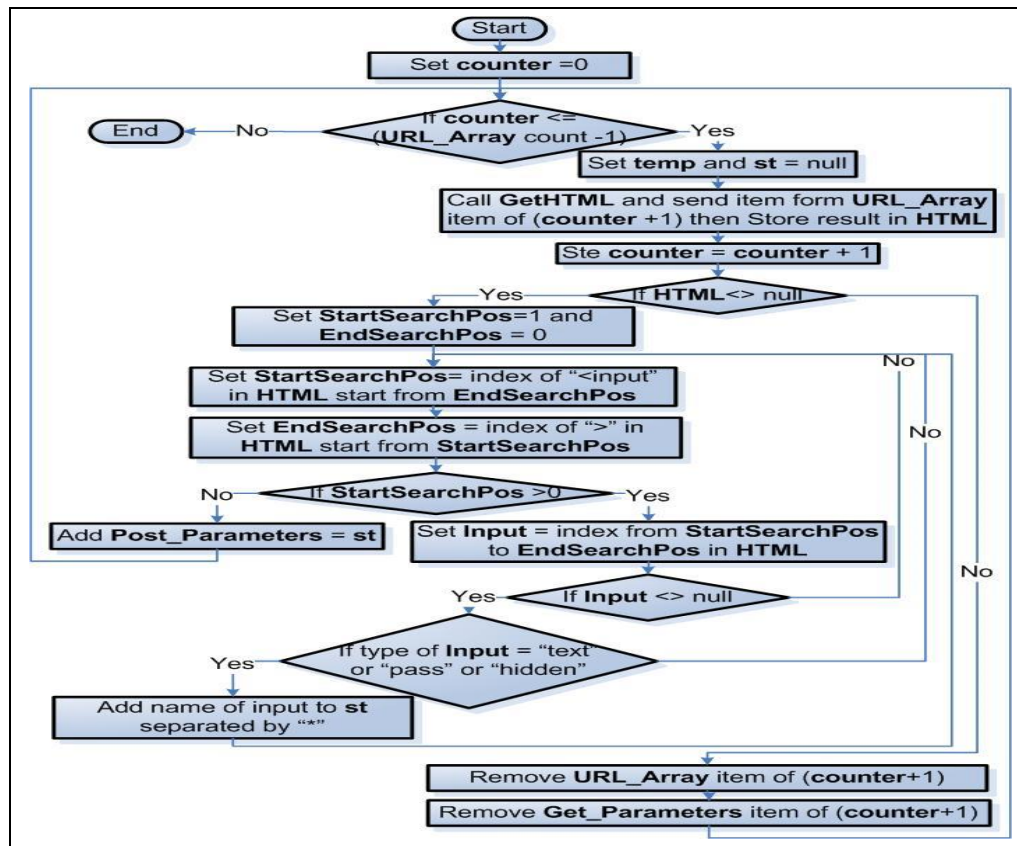


Fig. 3 Collecting the POST method parameters

Stage 2:

Detecting SQL injection stage is done by injecting vulnerable SQL statement like (') (single quotation) to the collected GET or POST methods and then analyze the response from the web server to see if there is an SQL Injection vulnerability or not.

III- Results and Discussion

Table 1 shows the web pages used for testing the proposed SQL detecting tool.

Table 1: The web pages used for testing the tool

No.	URL
1	http://www.google.com
2	http://www.facebook.com
3	http://www.moawiaelberier.com/
4	http://www.kremetgroup.com/index.php
5	http://www.saeedgroup.net/
6	http://citcsudan.org/
7	http://www.cgc-online.com/
8	http://localhost/ntcysite/
9	http://localhost/Jawhhara_Al-khartoum/

Figure 4 shows the main form of the SQL detecting tool users can input the URL to detect SQL injection the output will be the name of internal pages, GET, POST, button to preview the internal pages and button to alter the methods by SQL injection vulnerable statement variables .



Figure 4:Main form of the SQL detection tool

Table 2 shows the number of internal pages and the number of GET and POST methods for the tested pages as a results of running the proposed tool for three levels of the URL given in table 1.

Table 2: The results of the tested web pages in terms of (Internal pages, number of GET method and number of POST method)

No.	Domain Name	Discovered internal pages	GET	POST
1	http://www.google.com	142	95	267
2	http://www.facebook.com	113	40	1017
3	http://www.moawiaelberier.com/	8	0	0
4	http://www.kremetgroup.com/index.php	10	6	10
5	http://www.saeedgroup.net/	11	0	0
6	http://citcsudan.org/	19	0	28
7	http://www.cgc-online.com/	30	0	46
8	http://localhost/ntcysite/	56	6	88
9	http://localhost/Jawhhara_Al-khartoum/	22	0	10

From the table, the internal pages for Google and Facebook are relatively greater than other home pages. It is clear that number of POST method is greater than the number of GET method for all home pages. The tool is used to check these GET and POST methods by injecting them with vulnerable SQL statement.

Figure 5 shows the internal pages, GET methods, POST methods , preview and alter parameters for the home page http://localhost/ntcysite for the three levels. The preview button enables the users to open and preview the page immediately. The alter parameters used to inject SQL attacks likes ("1"="1', amin' --,admin', #admin'/*,' or 1=1--, ' or 1=1#, ' or 1=1/*).

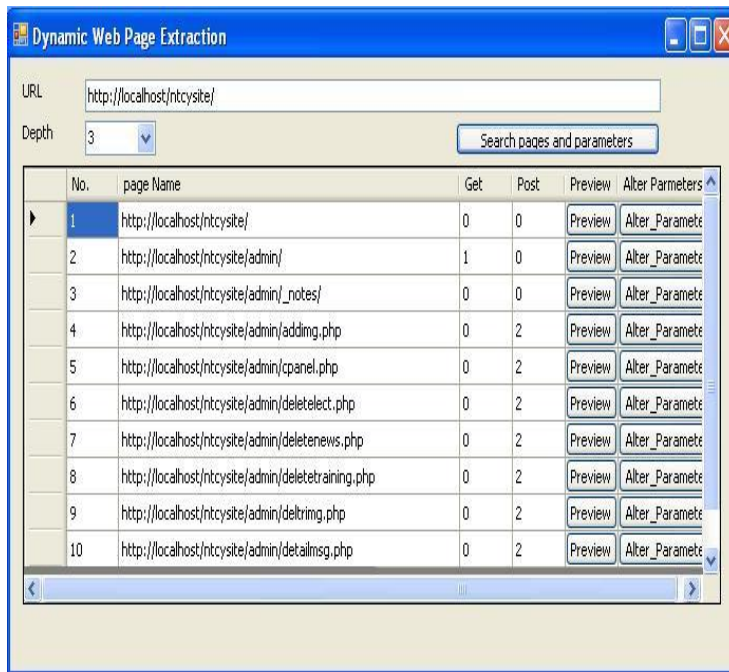


Figure 5: Dynamic web page extraction

The tool can alter GET and POST methods with SQL injection parameters. Figure 6 shows the actual admin form of the webpage <http://localhost/ntcysite/> without altering any parameters with SQL injection



Figure 6: Admin form of the homepage <http://localhost/ntcysite/>

Figure 7 shows the altering form for the parameter POST for the admin form of the homepage <http://localhost/ntcysite/> the result appear in figure 8 shows that the tool passes the admin restriction for the user name and password .

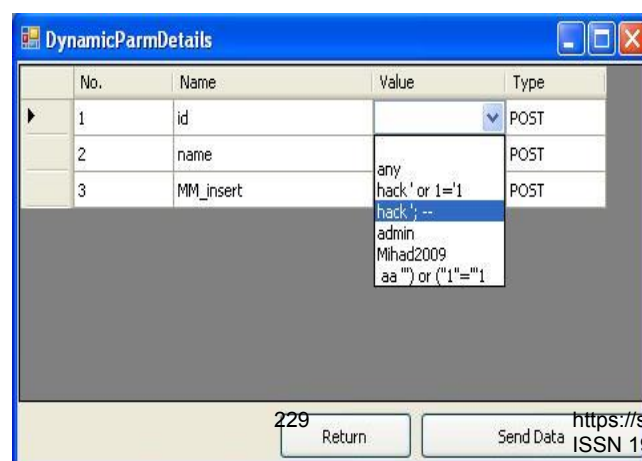


Figure 7: Altering GET or POST method

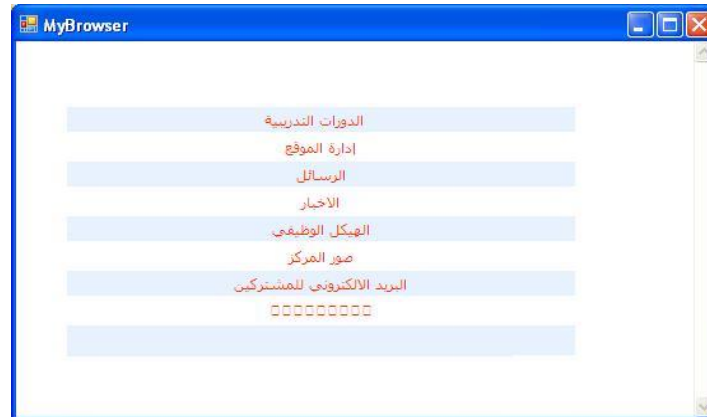


Figure 8: the form open after admin form

V- Conclusion

In this paper, the researchers have introduced a straightforward algorithm based on a tool to detect SQL injection vulnerabilities in the web applications online. Using this tool against real web applications under the administrative control can help to identify SQL vulnerabilities that an attacker could use to compromise a web application by altering SQL injection statements for the POST and GET methods. The tool gives good performance in detecting SQL injection vulnerability.

References

- [1] Atefeh Tajpour, Mohammad JorJor zade Shooshtari, "Evaluation of SQL Injection Detection and Prevention Techniques", Second International Conference on Computational Intelligence, Communication Systems and Networks, Jul. 2010.
- [2] Boyd, S. W., and Keromytis, A. D. Sqlrand: Preventing sql injection attacks. In ACNS (2004), pp. 292–302.
- [3] Buehrer, G., Weide, B. W., and Sivilotti, P. A. G. Using parse tree validation to prevent sql injection attacks. In SEM (2005).
- [4] Cesar Cerrudo. Manipulating Microsoft SQL server using SQL injection. Technical report, Application Security Inc., 2003.
- [5]. CERT Vulnerability Note VU#282403. <http://www.kb.cert.org/vuls/id/282403>, September 2002.
- [6] Chris Anley. Advanced SQL injection in SQL server application. Technical report, NGSSoftware Insight Security Research (NISR), 2002.
- [7] Debasish Das, Utpal Sharma, D.K. Bhattacharyya, " An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching", International Journal of Computer Applications, 2010, Volume 1 – No. pp. 25 28 .

- [8] Halfond, W., and Orso, A. AMNESIA, "Analysis and Monitoring for NEutralizing SQL-Injection Attacks." In ASE (2005), pp. 174–183.
- [9] Halfond, W., Orso, A., and Manolios, P., "Using Positive Tainting and Syntax-Aware Evaluation to Counter SQL Injection Attacks." In FSE (2006), pp. 175–185.
- [10] <http://www.programmerinterview.com/index.php/general-miscellaneous/html-get-vs-post> (visited on 14 Feb. 2015).
- [11] <https://www.cs.tut.fi/~jkorpela/forms/methods.html> (visited on 14 Feb. 2015).
- [12] Justin Clarke, "SQL Injection attacks and Defense ",Second Edition, ISBN: 978-1-59749-963-7, Copyright © 2012 Elsevier Inc.
- [13] Livshits, V. B., and Lam, M. S. Finding security vulnerabilities in Java applications with static analysis. In USENIX Security Symposium (2005).
- [14] Manveen Kaur,"SQL Injection Attacks - Its Prevention using Flag Sequencing Approach", Computer Engineering and Intelligent Systems ,SSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol.6, No.2, 2015.
- [15] Nguyen-Tuong, A., Guarnieri, S., Greene, D., Shirley, J., and Evans, D. Automatically hardening web applications using precise tainting. In SEC (2005), pp. 295–308.
- [16] OWASPD-Open Web Application Security Project. "Top ten most critical Web application Security Risks", https://www.o_sp.org/index.phpffop1020IO-Main
- [17] Pietraszek, T., and Berghe, C. V. Defending against injection attacks through context-sensitive string evaluation. In RAID (2005).
- [18] Puspendra Kumar, "A Survey on SQL Injection Attacks, Detection and Prevention Techniques", ICCCNT'12, 26th _28th July 2012, Coimbatore, India.
- [19] Ramya Dharam, Sajjan G. Shiva, "Runtime Monitoring Technique to handle Tautology based SQL Injection Attacks", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 189-203 The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012).
- [20] San-Tsai Sun_, Konstantin Beznosov, "SQLPrevent: E_ective Dynamic Detection and Prevention of SQL Injection Attacks Without Access to the Application Source Code ", technical report LERSSE-TR-2008-01
- [21] UK Security Breach Investigations Report An Analysis of Data Compromise Cases 2010.
- [22] Shakti Kumar, Subhendu Dey, R.Karthikeyan, K.G.S. Venkatesan, " Prevention of SQL Injection Attack on Web Applications", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 3, March 2015.
- [23] Sruthi Bandhakavi , Sruthi Bandhakavi , P. Madhusudan , V.N. Venkatakrishnan, "CANDID: Preventing SQL Injection Attacks using Dynamic Candidate Evaluations", CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA. Copyright 2007 ACM 978-1-59593-703-2/07/0011.
- [24] Su, Z., and Wassermann, G. The essence of command injection attacks in web applications. In POPL (2006), pp. 372–382.
- [25] Tajinderdeep Singh Kalsi, Navjot Kaur, "METHODS FOR PREVENTING SQL INJECTION ATTACKS:A REVIEW", International Journal of Advanced Engineering Technology, April-June,2015/08-1.
- [26] Udit Agarwal, Monika Saxena, Kuldeep Singh Rana, "A Survey of SQL Injection Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

- [27] Valeur, F., Mutz, D., and Vigna, G. A learning-based approach to the detection of sql attacks. In DIMVA (2005), pp. 123–140.
- [28] Xu, W., Bhatkar, S., and Sekar, R. Taint-enhanced policy enforcement: A practical approach to defeat a wide range of attacks. In 15th USENIX Security Symposium (2006).
- [29] Xie, Y., and Aiken, A. Static detection of security vulnerabilities in scripting languages. In USENIX Security Symposium (2006).
- [30] Yonghee Shin, Laurie Williams, Tao Xie, " SQLUnitGen: SQL Injection Testing Using Static and Dynamic Analysis", International Symposium on Software Reliability Engineering - ISSRE , 2006.

Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem

Shaligram Prajapat ¹(corresponding author) and Ramjeevan Singh Thakur²

¹Research Scholar, ² Associate Professor

Maulana Azad National Institute of Technology(MANIT) , Bhopal, INDIA

Abstract- This paper presents enhanced model of security of symmetric key based cryptosystem[1]. The enhancement of model by variable keys and key exchange using parameters only approach is also presented. The issue of fixing up the minimum length of key for AVK is also a big challenge in AVK model. Selection of shorter key length leads to vulnerability/compromise of system, on the other side, larger than optimum key size would involve unnecessary overheads and wastage of resources[2]. Further, ensuring high protection against malicious attack, is achieved through IDS software tools, that attempts to detect and prevent the system from malicious network users. Apart from these tools, various network security applications using pattern mining to extract the threat from cipher log. Faster and more efficient pattern matching algorithm to overcome the performance issue is demonstrated in[3], parameterized model of automatic variable key. Presented parameters only exchanged instead of key, has been analyzed using association rule discovery from hacker's perspective. This paper applies apriori method to investigate association rule among parameters used for generation of key and prediction of future key in the cryptosystem based on parameter only communication for AVK model[11]. In other words, the paper attempts to answer, How much the method is secure against association rule for future parameter prediction?

Index term: AVK, Symmetric Key, cryptosystem, IDS, Parameterized model

I. INTRODUCTION

In recent era exchange of all the information including financial and e-commerce transaction takes place among parties or entities that might not known to each other but participates in communication. During this transmission of information public network is used hence ensuring the security of these information and confidentiality of involved parties is mandatory. The information stored in computers or during information, to avoid unauthorized access or damage of information technique known as Encryption and Decryption mechanism is used. Before transmission of information Encryption and after receiving of information Decryption process is used[1].

Securing information based on used key is classified into symmetric, asymmetric or hash. If both sender and receiver use the same key then it is symmetric cryptosystem. And if encryption and

decryption key are different then it is known as asymmetric cryptosystem. In any of the situation, the used key decides the level of security of cryptosystem. There are various alternatives to control the security of a cryptosystem like Hind the Encryption, Decryption algorithms. But by doing reverse engineering if the behavior of algorithm is known then whole cryptosystem will fame. Or by increasing the key size [6] (Increasing the key size will result in increase in key guess time or by increasing brute force attack time/trials that ultimately will increase the system security. But increasing the key size will increase the time in encryption or decryption process .By increasing computing resources or energy required to process will definitely be affected once the key length has been increased beyond a threshold[5]. Hacker or cryptanalyst may use parallel processing; multiword computing and advanced algorithms usage may lead to compromise the system security.

Another alternative in this direction we fixed up the key with a specific length and try to vary it from session to session. This approach forms the basis of self variable key based AVK-Model, In this AVK model as we fixed up the length of key to a minimum threshold then the number of resources are freed. Up. Since the key varies from session to session so if hacker or cryptanalysis gains the access of key of a particular session even though it is invalid for next session. So the level of security of cryptosystem is enhanced. In AVK model. since the key changes from session to session, so the issue of new key exchange arises .To handle this issue we apply parameters AVK model that exchanges only parameters for key generation. Since on the public network only parameters are exchanged, so both sender and receiver will computer key at their own end and construct the key.

The AVK approach with parameterized model is to be investigated from the perspective of hackers or cryptanalyst. The detailed analysis will decide the success of the AVK model of symmetric cryptosystem. This analysis is termed as Cryptic Mining[8,12]. Cryptic mining as a set of cryptic algorithm [2,3,4]that analyses the captured plaintext-cipher text, plaintext-key logs, parameters-key logs and captured cipher logs and provides useful knowledge, process and developing the knowledge based or AI based framework[8]. In future cryptic mining algorithm group will be useful for auditing and classification of cryptic algorithms. Theoretically cryptic algorithms provides random ciphers, but in practice it is not so, these algorithm uses pseudo random numbers that are generated by some computer or mathematical formula. So these ciphers have some sort of patterns, by extracting these patterns cryptic mining algorithms may find possible sequence or hints about key or association among key and plaintext or cipher. Depending upon the degree of patterns in the output the class of cryptic algorithms can be decided[2]. In this way, in future AVK algorithm may contribute in the extension of symmetric algorithm design. Certainly this provide strength to mechanism of maintenance and exchange of information.

According to Moore's law the power of personal computers has historically doubled approximately every 18 months what is the effect of this growth on key prediction and key computation? Obviously for high security, cryptography domain recommends that length of key must be kept sufficiently large to prevent form systematic attack the length of key is also increasing with passage of time. Moreover, cryptanalyst or hacker is well equipped with latest

techniques, devices and powerful algorithms to exploit threats or efficacy of key search attacks [5,8]. Therefore, estimates of the time required for successful key search attacks must be revised downward as the computing power and resources available to attacker's increases. AVK approach of cryptography can be a better alternative in this direction. For immixing the threats of key leakage, instead of key exchanged some parameters can be exchanged that would be sufficient for construction of key for both Alice and Bob. As parameters only are exchanged so the security of the system would not be compromised.

In the next sections, some related work has been presented for symmetric cryptosystem, Then parameterized model of AVK process has been discussed. The success of this model has been investigated with association rule discovery of cryptic mining technique. This cryptanalysis perspective for extraction of key parameters using one of the popular techniques of cryptic mining as association rule discovery does auditing of cryptosystem. The same has been checked from WEKA tool. At the end other technique of cryptic mining has been pointed out.

II. BACKGROUND

Encryption: Database of important and Sensitive information such as: Credit card information, passwords, financial data etc. are made difficult to understand by man in middle this essential process is used. It uses a secret key is used to transfer text; audio or video is converted in to non understandable form. Input file that is to be secured is popularly known as plain text. And transformed file that has been enciphered is known as cipher text or cryptogram.

Decryption: The received encrypted file is transformed back to understandable form using key is known as decryption.

Apart from privacy preservation domain [1], data mining techniques are being explored for applicability in cryptographic domain. In [2, 8, and 9] classification method of encrypted text is attempted, in [3] machine learning domain also has been related with data mining algorithm tasks. Various symmetric key cryptographic algorithms have been compared for different key length and available in literature. Data Mining Techniques [4, 5, 6, and 7] for cryptographic domain has been discussed and needs to be explored in greater depth further. Recently, in [11, 12, 13] AVK approach has been discussed with Fibonacci –Q matrix, sparse based schemes. In [14] automatic variable key under various approaches in cryptographic system has been analyzed. In this research community P. Chakrabarti has proposed approaches of key computation using parameters using fuzzy concepts [10]. This AVK approach can be further improved for enhancing security level. This can be achieved by parameter -only exchange of information. The scheme is reviewed from the perception of cryptanalyst for association rule inference. The subsequent sections 3, 4, 5 respectively presents the model with illustration of simply mean based method and later on it is analyzed in the light of association rule mining.

III. PARAMETER BASED COMMUNICATION SCHEME

This section presents Scheme of Parameters exchange only for secure communication for automatic variable key. Consider sample algorithm-1 and 2, to demonstrate working of information exchange based on parameters only scheme in fig. - 1.

Algorithm-1 parameters4Key-Alice (parameters x_1, x_2, \dots, x_m)

```
{
1. Read parameters  $x_1, x_2, \dots, x_m$ ;
2. Compute the key for information exchange by:  $\text{key}_i = (x_1 * x_2 * \dots * x_m)^{1/2}$  ;
3. Sense the information to exchange= $D_i$  ;
4. If (mode==transmit)
    Generate Cipher text  $C_i = \text{Encrypt}(D_i, \text{key}_i)$ ;
    Transmit  $C_i$ ;
5. else
    Receive Plain text  $P_i = \text{Decrypt}(D_i, \text{key}_i)$ ;
    Use  $P_i$ ;
}
```

Algorithm-2 Parameters4Key-Bob (parameters x_1, x_2, \dots, x_m)

```
{
1. Receive parameters  $x_1, x_2, \dots, x_m$ ;
2. Compute the Arithmetic Mean  $A.M. = (x_1 + x_2 + \dots + x_m)/2$ ;
3. Compute the Harmonic Mean  $H.M. = 2 * x_1 * x_2 * \dots * x_m / (x_1 + x_2 + \dots + x_m)$ 
4. Compute the Key  $i = (A.M * H.M)^{1/2}$ 
5. If (mode==transmit)
    {
        Generate Cipher text  $C_i = \text{Encrypt}(D_i, \text{key}_i)$ ;
        Transmit  $C_i$ ;
    }
6. else
    Receive Plain text  $P_i = \text{Decrypt}(D_i, \text{key}_i)$ ;
    Use  $P_i$ ;
}
```

These algorithms have following advantages over traditional key exchange algorithm.
(1) Without exchanging entire key Alice and Bob will securely communicate with each other.
Without exchanging entire key Alice and Bob will securely communicate with each other. (2) In

this model keys are computed using different functions, which also enhance level of security. At Node A:

1. Compute $k_1 = \text{A.M. of Parameters } \{p_1, p_2, \dots, p_k\}$
2. Compute $k_2 = \text{Harmonic Mean of Parameters } \{p_1, p_2, \dots, p_k\}$
3. Compute product $p = p_1 * p_2 * \dots * p_k$
4. Compute $\text{Key} = \sqrt{p}$
5. Use key for sending and receiving information.

And at node-B:

1. Compute product of parameters $= p$ i.e. $\{p_1, p_2, \dots, p_k\}$
2. Compute $\text{Key} = \sqrt{p}$ where $p = \{p_1, p_2, \dots, p_k\}$
3. Use key for sending and receiving information

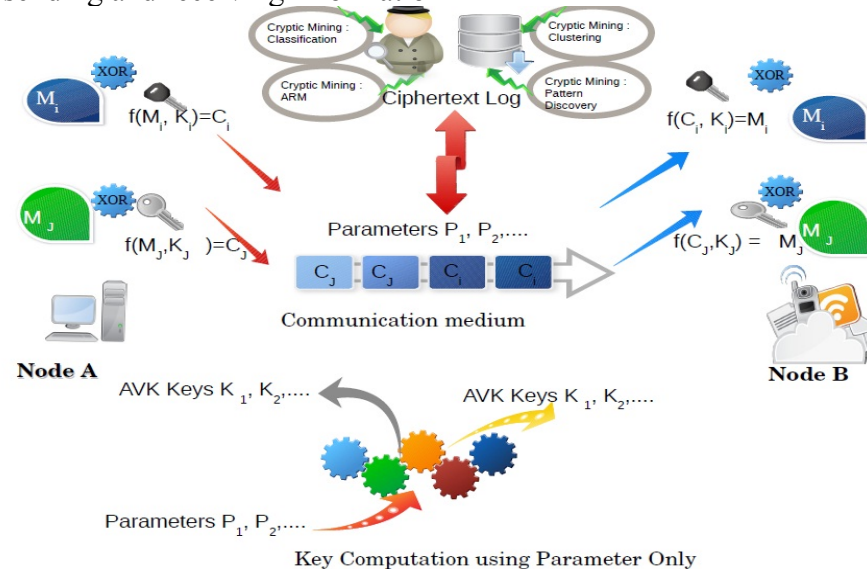


Fig 1: Secure communication scheme using Parameter exchange

IV. ASSOCIATION RULES FOR PARAMETER EXCHANGE SCHEME

Conventionally association rule $\text{Key} \rightarrow \text{Parameter}$ sets indicates that if Key (antecedent) appears then Parameter set (consequent) p_i, p_j, \dots, p_k also tends (with highly probable) to appear, where X and Y may be single parameters or set of parameters (in which the same parameter does not appear in both sets) in other words X and Y would be found together frequently in the given training set and they does not show a causal relationship.

Notations: The number of parameters in session table is n. Key of a particular session is constituted from parameter terms from key $\{p_i, p_j, \dots, p_k\}$ and it is denoted by $f(p_i, p_j, \dots, p_k)$ where p_i, p_j, \dots, p_k are variables specific to a particular session. Further, assume that there are n-sessions information is available ($n=10$, for session-parameter table). Each session of this table is

denoted by $S = \{ S_i, S_j, \dots, S_k \}$ with a unique session-Id, specifying a set of parameter constituting the key (possibly a small subset). Each session key of m parameters be with key $K_i = \{ p_i, p_j, \dots, p_k \}$.

Typically session key is varied due to differences in the number of parameters. The goal of cryptanalyst here is to find association relationships from a given large number of session keys, such that parameters that tend to occur together are identified. As Cryptanalyst has record of what each session key parameters used for generally session keys. In table 1.1 each row of the table gives the set of parameters that may be used in sessions.

Table 1: Session wise parameters of key

Session No.	Key	Key Parameters
S ₁	$SK_1 = f(p_1, p_2, p_8)$	p_1, p_2, p_8
S ₂	$SK_2 = f(p_1, p_2, p_4)$	p_1, p_2, p_4
S ₃	$SK_3 = f(p_1, p_5)$	p_1, p_5
S ₄	$SK_4 = f(p_2, p_3, p_4, p_5)$	p_2, p_3, p_4, p_5
S ₅	$SK_5 = f(p_3, p_6, p_7, p_8, p_9)$	p_3, p_6, p_7, p_8, p_9
S ₆	$SK_6 = f(p_3, p_4, p_5, p_7, p_8, p_9)$	$p_3, p_4, p_5, p_7, p_8, p_9$
S ₇	$SK_7 = f(p_1, p_2)$	p_1, p_2
S ₈	$SK_8 = f(p_1, p_2, p_3, p_4)$	p_1, p_2, p_3, p_4
S ₉	$SK_9 = f(p_1, p_5)$	p_1, p_5
S ₁₀	$SK_{10} = f(p_1, p_3, p_4, p_5, p_6, p_8, p_9)$	$p_1, p_3, p_4, p_5, p_6, p_8, p_9$

Cryptanalyst would be interested to find which parameters set are used frequently in a session table. Say, p_9, p_6 are the two parameters that are used together frequently then the hacker may start predicting by having one parameter information, in the hope that the second parameter information can be found by obtained association rule. Given a large set of transactions, we seek a procedure to discover all association rules which has at least $p\%$ support with at least $q\%$ confidence such that all rules satisfying these constraints are found in efficient manner. Out of these rules we are also interested to find rules that are practical or actionable.

V. APRIORI APPROACH FOR PARAMETER PREDICTION

Consider a Transaction log with information about 25 session i.e. $S = \{ S_1, S_2, \dots, S_{25} \}$ with

exchanging the key using parameters only method from parameter space of 16 possibilities i.e. $P=\{p_1, p_2, \dots, p_{16}\}$. A key of a particular session will be random selection of some parameters from P and then applying secret algorithm to compute key of that particular session. In the automatic variable key environment, We assume that cryptanalyst or hacker somehow recorded traces of parameters used in few sessions say 25, without the information of function he may be interested to know the frequent parameters or guessing future parameters based on association rules, applied on these parameter to recomputed the future key session.

Table 2. Transaction log containing parameter traces

S ₁	p ₁ , p ₂ , p ₄ , p ₆ , p ₁₆
S ₂	p ₁ , p ₃ , p ₄ , p ₆
S ₃	p ₄ , p ₅ , p ₇ , p ₉ , p ₁₀
S ₄	p ₂ , p ₄ , p ₆ , p ₃ , p ₉
S ₅	p ₂ , p ₃ , p ₅ , p ₇ , p ₉
S ₆	p ₁₀ , p ₁₅
S ₇	p ₁ , p ₂ , p ₄ , p ₆ , p ₁₀
S ₈	p ₈ , p ₁₀ , p ₁₅
S ₉	p ₂ , p ₃ , p ₄ , p ₅ , p ₆
S ₁₀	p ₂ , p ₃ , p ₅ , p ₇ , p ₉
S ₁₁	p ₂ , p ₄ , p ₉
S ₁₂	p ₂ , p ₄ , p ₆ , p ₇ , p ₉
S ₁₃	p ₁ , p ₂ , p ₃
S ₁₄	p ₃ , p ₄ , p ₅ , p ₇ , p ₉
S ₁₅	p ₅ , p ₆
S ₁₆	p ₇
S ₁₇	p ₇ , p ₈ , p ₉
S ₁₈	p ₁ , p ₂ , p ₄ , p ₆
S ₁₉	p ₂ , p ₃ , p ₅ , p ₇ , p ₉
S ₂₀	p ₄ , p ₅ , p ₇ , p ₉
S ₂₁	p ₁₀ , p ₁₅ , p ₁₆
S ₂₂	p ₂ , p ₃ , p ₄ , p ₆
S ₂₃	p ₅ , p ₇ , p ₉ , p ₁₀ , p ₁₁
S ₂₄	p ₁₁ , p ₁₂ , p ₁₃
S ₂₅	p ₁₃ , p ₁₄ , p ₁₅

The frequency of each parameter in the session logs is given in following set, where set element={parameter, frequency of parameter} is listed below: $\{\{p_1:4\}, \{p_2:13\}, \{p_3:10\}, \{p_4:11\}, \{p_5:9\}, \{p_6:9\}, \{p_7:10\}, \{p_8:2\}, \{p_9:11\}, \{p_{10}:6\}, \{p_{11}:2\}, \{p_{12}:1\}, \{p_{13}:2\}, \{p_{14}:1\},$

$\{p_{15}:4\}, \{p_{16}:2\} \}$

Phase-1: Computation of frequent set

.Assuming support of parameters (25% supports in 25 sessions) to occur in at least 7 sessions for computing first frequent parameter sets L_1 :

Table 3. L_1 : First frequent parameter set

Parameter	P ₂	p ₃	p ₄	p ₅	p ₆	p ₇	p ₉
Frequency	13	10	11	9	9	10	11

Computation of C_2 : There are 21 candidates for, 2-parameter set of C_2

$\{(p_2, p_3), (p_2, p_4), (p_2, p_5), (p_2, p_6), (p_2, p_7), (p_2, p_9), (p_3, p_4), (p_3, p_5), (p_3, p_6), (p_3, p_7), (p_3, p_9), (p_4, p_5), (p_4, p_6), (p_4, p_7), (p_4, p_9), (p_5, p_6), (p_5, p_7), (p_5, p_9), (p_6, p_7), (p_6, p_9), (p_7, p_9)\}$

Table 4: C_2

parameter set	Frequency
(p ₂ ,p ₃)	9
(p ₂ ,p ₄)	8
(p ₂ ,p ₅)	4
(p ₂ ,p ₆)	8
(p ₂ ,p ₇)	4
(p ₂ ,p ₉)	6
(p ₃ ,p ₄)	5
(p ₃ ,p ₅)	4
(p ₃ ,p ₆)	5
(p ₃ ,p ₇)	4
(p ₃ ,p ₉)	6
(p ₄ ,p ₅)	4
(p ₄ ,p ₆)	9
(p ₄ ,p ₇)	3
(p ₄ ,p ₉)	4
(p ₅ ,p ₆)	1
(p ₅ ,p ₇)	7

(p ₅ ,p ₉)	7
(p ₆ ,p ₇)	1
(p ₆ ,p ₉)	2
(p ₆ ,p ₉)	9

Table 5. L₂: The frequent 2-parameter set

(p ₂ ,p ₃)	9
(p ₂ ,p ₄)	8
(p ₂ ,p ₆)	8
(p ₄ ,p ₆)	9
(p ₅ ,p ₇)	7
(p ₅ ,p ₉)	7
(p ₇ ,p ₉)	9

Table 6. C₃: candidate Sets of 3- parameter set and frequency

Candidate set 3-parameter set	Frequency
p ₂ , p ₃ , p ₄	4
p ₂ , p ₃ , p ₆	4
p ₂ , p ₄ , p ₆	8
p ₅ , p ₇ , p ₉	7

Table 7. L₃: 3-frequent-parameter set

3-frequent - parameter set	Frequency
p ₂ , p ₄ , p ₆	8
p ₅ , p ₇ , p ₉	7

Phase-2 Computation of association rule

We compute 3-frequent-parameter set i.e. L₂, Taking one parameter in antecedence from {p₂, p₄,

$p_6\}$ we get:

$$\{ p_2 \rightarrow p_4, p_6 : p_4 \rightarrow p_2, p_6 : p_6 \rightarrow p_2, p_4 \}$$

Rules with 2-parameter set in antecedence position

$$\{ p_4, p_6 \rightarrow p_2 : p_2, p_6 \rightarrow p_4 : p_2, p_4 \rightarrow p_6 \}$$

Taking support =8 computation of Confidence of association rules for parameters p_2, p_4, p_6 are given in following table 7.

Table 8. Association rules for p_2, p_4, p_6

Rule	Support of (p_2, p_4, p_6)	Frequency of Antecedence	Confidence
p_2, p_4, p_6	8	13	0.61
p_4, p_2, p_6	8	11	0.72
p_6, p_2, p_4	8	9	0.89
$p_4, p_6 \rightarrow p_2$	8	9	0.89
$p_2, p_6 \rightarrow p_4$	8	8	1
$p_2, p_4 \rightarrow p_6$	8	8	1

With support =7, computation of confidence for p_5, p_7, p_9 is shown in following table:

Table 9. Association rules for p_5, p_7, p_9

Rule	Support	Frequency of Antecedent	Confidence
p_5, p_7, p_9	7.0	9	0.78
p_7, p_5, p_9	7.0	10	0.7
p_9, p_5, p_7	7.0	11	0.64
p_7, p_9, p_5	7.0	9	0.78
p_5, p_9, p_7	7.0	7	1
p_5, p_7, p_9	7.0	7	1

Results: With confidence=0.7 cryptanalyst or hacker may infer all-7 rules (without rule number 3). So 5 of them also satisfy after checking L_2 also we get $p_2 \rightarrow p_3$ and $p_3 \rightarrow p_2$ and they both have confidence. $p_4 \rightarrow p_2, p_4 \rightarrow p_6, p_6 \rightarrow p_2, p_6 \rightarrow p_4, p_4, p_6 \rightarrow p_2, p_2, p_6 \rightarrow p_4, p_2, p_4 \rightarrow p_6, p_5 \rightarrow p_7,$

$p_5 \rightarrow p_9$, $p_7 \rightarrow p_5$, $p_7 \rightarrow p_9$, p_7 , $p_9 \rightarrow p_5$, p_5 , $p_9 \rightarrow p_7$, p_5 , $p_7 \rightarrow p_9$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_2$; (rules have been decomposed like $p_4 \rightarrow p_2$, p_6 by two rules $p_4 \rightarrow p_2$, and $p_4 \rightarrow p_6$).

VI. EXPERIMENTAL SETUP

In order to verify association rule using WEKA-64 bit tool kit, we compare association rule obtained from analytical method with corresponding rules generated from WEKA. The same can be generalized and verified for more number of parameters and session logs. The Run information is elucidated below: For hypothetical input session in Table 10 results are in Table 11. The same is computed from WEKA tool elucidate in table 12. Obviously, output of association process has been presented in the format $X \Rightarrow Y$. The count associated with the antecedent = absolute coverage in the dataset. The number next to the Y = absolute number of instances that match the X and the Y . The number in brackets on the end is the support for the rule (no. of X divided by the number of matching consequents).

Table 9. Session wise parameters for AVK

Session ID	Parameters for Key
S1	p_1, p_2
S2	p_1, p_2, p_4
S3	p_1, p_5
S4	p_2, p_4, p_5

Table 9. Association rules with confidence

Possible Rule	Confidence	Desirable confidence
$p_1 \rightarrow p_2$	2/3	< 0.75
$p_2 \rightarrow p_1$	2/3	< 0.75
$p_2 \rightarrow p_4$	2/3	< 0.75
$p_5 \rightarrow p_2$	3/3	> 0.75

Table 9. WEKA Result

S.No .	Scheme	Weka .associations .Apriori -N 10 -T 0 -C 0.9 -D 0.05 -U 1.0 -M 0.1 -S -1.0 -c -1
1.	Relation	R
2.	Instances	4
3.	Attributes	4
4.	Parameters	p_1, p_2, p_4, p_5
5.	Using Apriori	Size of set of large item sets L(1): 4

	generated rule base	Size of set of large item sets L(2): 6 Size of set of large item sets L(3): 2
6.	Best rules found Minimum support: 0.25 (1 instances) Minimum metric <confidence>: 0.9 Number of cycles performed: 15	1. $p_4=t_2 \implies p_2=t_2$ conf:(1) 2. $p_1=t_4 \implies p_2=t_1$ conf:(1) 3. $p_4=t_5 \implies p_2=t_1$ conf:(1) 4. $p_2=t_5 \implies p_4=t_1$ conf:(1)

So one can say that a cutoff of 50% was used in selecting rules, of “Association rule generation” window and indicated in that no rule has coverage less than 0.50. This aligns with analytical result. So the association rules can be extracted for large number of parameter set and cryptanalyst may generate rule based for key computation.

VII. FUTURE ENHANCEMENT

Apart from association rule the model is to be tested for following cryptic mining techniques. (1) Statistical-Cryptic Pattern: Using statistical inferences, accurate notification of malicious activities that are appearing over several time periods acts as indicators of inferring denial-of-service attacks. Challenging task is to determine thresholds to balance the errors and probability of false positive/negative results. It is desirable to have accurate statistical distributions; further challenge is to model all behavior purely using statistical methods. The statistical cryptic pattern identification attempts with features only without consider the relations between features. (2) Cryptic Clustering: IDS-cryptic clustering is to learn from and detect intrusions without requiring the explicit descriptions of various attack classes. The common methods are hierarchical clustering and partition clustering. (3) Fuzzy approach: Using Boolean boundary the intrusion data are partitioned into the interval, with sharp boundary problem for cipher classification. The concept of fuzzy logic uses partial membership among items of set to integrate with the association rules and frequent patterns may provide different insights of cipher logs (abstraction and generalization). (4) Artificial Neural Networks (ANN): Concept of Artificial Neural Network (ANN) supports to design useful nonlinear classifiers of cryptosystems (m- inputs and n-outputs), based on instances of input-output relationship (such as plain text –cipher text pairs). with minimum priory knowledge, and sufficient layers and neurons. (5) Structural Pattern Recognition: using the patterns and structure of plain text –cipher text information, Structural pattern recognition (Syntax and structure) finds some simple sub-patterns that composes longer pattern. The basis of syntax analysis is theory of formal language (handles with symbol information) and of structure analysis is some special technique of mathematics based on sub-patterns (static classification or artificial neural networks). (6) Support Vector Machine (SVM): Support Vector Machine is an effective tool for cryptic pattern recognition. (7) Approximate reasoning approach: Combined fuzzy and compositional rule of inference approach may be used to

generate rule based pattern identification.

VIII. CONCLUSION

This paper examines novel scheme of secure information exchange over the network that may be useful for effective systems. AVK approach is to be tested on real implementation using secured parameter based communication adding extra security feature in the system. Association rule for predicting probable parameters from parameter space using association rule may provide hints for future parameters to predict key. But since both number of parameters as well as key of session is variable and changing from session to session, so the security of the system would not be compromised with the automatic variable scheme. Cryptic pattern identification influenced by a lot of methods from numerous domains. Apart from association rule discovery, other techniques of cryptic mining needs to be examined and implemented.

REFERENCES

- [1]. Shaligram Prajapat, R.S. Thakur, (2014).Time variant approach towards symmetric key. SAI-Conference London. Cosponsored by IEEE.
- [2]. Shaligram Prajapat ,R. S. Thakur(2015).Optimal Key Size of the AVK for Symmetric Key Encryption.CJICT,2015.
- [3]. Rivets (1993).Cryptography and machine learning. In Advances in Cryptology—ASIACRYPT'91.
- [4]. Dunham H (2008).Data Mining: Introductory and Advanced Topics. Pearson education: p.p.-4.
- [5]. Shaligram Prajapat, G. Parmar, R. S. Thakur (2015).Investigation For Efficient Cryptosystem Using SGcrypter.IJAER.pp.853-858
- [6]. Saxena G., Karnik H., Agawam M. (2008). Classification of Ciphers using Machine learning
- [7]. Rao B. M.(2003). Classification of RSA and IDEA Ciphers.
- [8]. Shaligram Prajapat. Thakur. Maheshwari,R. S. Thakur(2015).Cryptic Mining in Light of Artificial Intelligence. DOI: 10.14569/IJACSA.2015.060808.
- [9]. Shaligram Prajapat, R.S. Thakur. (2015). Various Approaches towards Cryptanalysis. International Journal of Computer Applications. 127(14):15-24, October 2015. Published by: Foundation of Computer Science (FCS), NY, and USA.doi: 10.5120/ijca2015906518.
- [10]. P. Chakrabarti (2008).Key Generation in the Light of Mining and Fuzzy Rule. IJCSNS.
- [11]. Shaligram Prajapat, Amber Jain, R. S. Thakur,(2012) A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix. www.interscience.in, IJCCT, Vol.3, Issue 3.

- [12]. Shaligram Prajapat, Ramjeevan Singh Thakur (2015). Cryptic-Mining: Association Rules Extractions Using Session Log. Computational Science and Its Applications. proceeding of ICCSA 2015. Volume 9158 of the series Lecture Notes in Computer Science pp 699-711
- [13]. Shaligram Prajapat, R.S. Thakur et al. (2014). Sparse approach for realizing AVK for Symmetric Key Encryption. IJRDET and in proceeding of International Research Conference on Engineering, Science and Management (IRCESM) Dubai, UAE.
- [14]. Goswami R., Chakrabarti S., Bhunia A., Bhunia C.(2014.). Generation of automatic variable key under various approaches in cryptographic system. J. Institute of Engineers India.
- [15]. Shaligram Prajapat, R.S. Thakur. (2016). Cryptic Mining for Automatic Variable Key based Cryptosystem. Procedia Computer Science. Elsevier.

Assessment of revenue in roadside units (RSU) in traffic management

Arefe Esalat Nejad^{1,*}

¹Young Researchers and Elite Club, Baft Branch, Islamic Azad University, Baft, Iran.

*corresponding Author

ABSTRACT

Vehicular networks, besides supporting safety-oriented applications, are nowadays expected to provide effective communication infrastructure also for supporting leisure-oriented application including content sharing, gaming and Internet access on the move. This work focuses on Vehicle to Infrastructure (V2I) scenarios, where multiple content providers own a physical infrastructure of Road Side Units (RSUs) which they use to sell contents to moving vehicles. This paper studies a relevant problem in VANETs, known as the deployment of Roadside Units (RSUs). A RSU is an access points, used together with the vehicles, to allow information dissemination in the roads. Knowing where to place these RSUs so that a maximum number of vehicles circulating is covered is a challenge. We model the problem as a Maximum Coverage with Time Threshold Problem (MCTTP), and use a genetic algorithm to solve it.

Keywords: Vehicular Network, RSU, Traffic Management, VANET.

1. INTRODUCTION

The constant increase in the number of cars traveling along the roads worldwide calls for effective means to improve the road safety and the efficiency of the overall transportation infrastructure. To this end, the research community, the industries and the governments all over the world are investing much of their efforts and money on the development of integrated Intelligent Transportation Systems (ITS) based on wireless communication networks allowing vehicles, equipment on the road, service centers and intelligent sensors to exchange information in a prompt and cost effective way. A Vehicular Ad Hoc Network (VANET) (Hartenstein et al., 2008; Li and Wang, 2007; Yousefi et al., 2006) is a network where each node represents a vehicle equipped with wireless communication technology. Communication in these networks can be Vehicle-to-Vehicle (V2V), when vehicles communicate directly, or V2I (Vehicle-to Infrastructure), when vehicles exchange information with access points, called Roadside Units (RSUs), and any other network infrastructure, such as 3G and 3GPP Long Term Evolution (LTE). VANETs are able to collect real-time data on road conditions and make them useful for a wide range of applications, including safety-warning systems, drivers' assistance and traffic routing (Toor et al., 2008). Successful deployment of vehicular ad hoc networks (VANETs) where information (such as traffic, road information or safety messages) is sent, forwarded, and received by vehicles depends on the adoption of the new wireless technology, namely the Dedicated Short Range Communications (DSRC) technology. Since it is anticipated that the DSRC technology might be a mandate for modern vehicles effective 2017, with high probability, vehicle-to infrastructure (V2I) communications-based networks will be the first type of vehicular ad hoc networks (VANETs) that might be implemented and, as such, they could accelerate the adoption of the DSRC technology.

VANETs are able to collect real-time data on road conditions and make them useful for a wide range of applications, including safety warning systems, driver's assistance and traffic routing. This last information, for instance, could be used to create vehicle routes according to carbon emission levels, avoiding routing certain types of vehicles to polluted areas. Moreover, these data can be used to create intelligent traffic management systems, which can automatically update traffic light cycles, indicate probable urban tolling zones, study the daily population of vehicles in the road, etc. Despite all the advantages VANETs can offer to road transport, there is currently a lack of studies on energy efficient (green) communication on VANETs (Toutouh and Alba, 2011). Among others issues, Green Communication involves information dissemination (Bakhouya et al., 2011; Lochert et al., 2009). In scenarios such as the ones showed in Figure 1, information dissemination is a crucial aspect. Apart from the vehicles, RSUs are especially important agents of information dissemination, because they deal with VANETs characteristics that can make communication hard, such as high mobility, dynamic topology and latency. Given a specific scenario, defining how many RSUs are necessary and where they will be deployed is a challenge. What we want is to use the minimal number of RSUs with the maximum possible coverage of the region (and consequently, vehicles) being considered. This problem of where to deploy RSUs that will participate on a VANET can be modeled using different variations of the set coverage problem (Trullols et al., 2010).

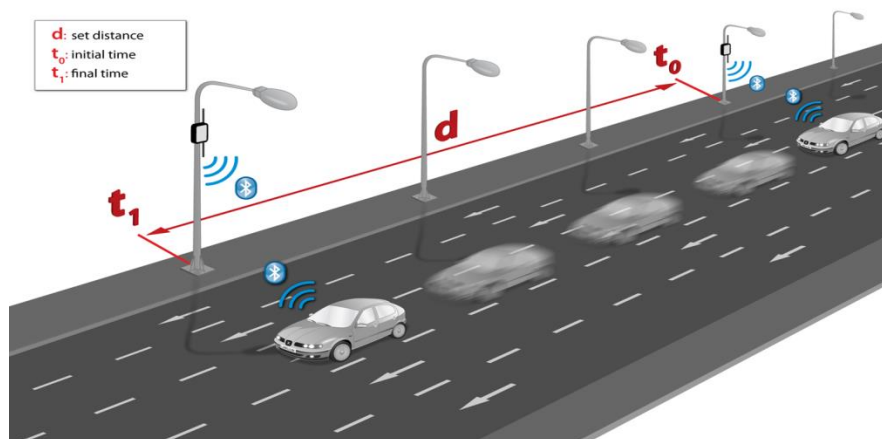


Fig.1. Libelium's Vehicle Traffic Monitoring Platform enables system

For instance, presented three different models and many solutions for the problem, including Maximum Coverage Problem (MCP), Knapsack Problem (KP), and Maximum Coverage with Time Threshold Problem (MCTTP). Their results showed MCTTP as an effective approach, and hence this is the model used in this paper. However, instead of using local search methods, we take advantage of the global search of a Genetic Algorithm (GA) to find the positions of the RSUs, and compare the results with the ones obtained by a greedy approach, which achieved the best results in (Trullols et al., 2010; Macedo et al., 2012).

2. HISTORY OF VANET

A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. It is estimated that the first system that will integrate this technology are police van, ambulance and fire vehicles to communicate with each other for safety purpose. Automotive companies like General

motors, Toyota, Nissan, DaimlerChrysler, BMW and Ford promote this term. Intelligent vehicular ad hoc network (In VANET) is another term for promoting vehicular networking. In VANET integrates multiple networking technologies such as Wi-Fi, IEEE 802.11p, wave IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA and ZigBee.

3. Interpretation Problem

The U.S. Department of Transportation (DoT) was expected to have a nationwide deployment of the roadside infrastructure in 2008. This plan, however, did not materialize and, to date, very few RSUs have been deployed. Major reasons that prevented the success of the plan can be summarized as follows:

- ✓ Justifying the benefits that RSUs provide is difficult
- ✓ Global cooperation and partnership with private sector
- ✓ Funding approaches

Ermining the value of such a radical proposition in uncertain future markets has proven to be nontrivial and fairly complicated. Even though the benefits of V2V and V2I systems in terms of safety, traffic efficiency, and environment are clear and have been reported in, the full benefits of the DSRC technology cannot be realized unless the technology is widely adopted by the market. These existing systems provide both safety and traffic efficiency benefits (i.e., roadside assistance help alert drivers of slow vehicles ahead and/or upcoming work zone while a transportation and traffic information telephone hotline allows travelers to choose the most efficient mode and route to their final destination). Proven effectiveness, high user satisfaction, existing widespread deployment, and already-invested capital into the existing systems have further impeded the nationwide deployment of RSUs.

4. Pervious Work

The deployment of sensors in wireless networks to improve communication is a classic issue in Wireless Sensor Networks (WSNs), and many authors have proposed solutions based on a variety of methods to tackle it (Filippini et al., 2012). Huang and Tseng formulated the coverage problem as a decision problem where, given a number k , the goal was to determine

Whether at least k sensors covered the area served by the sensor network. They proposed polynomial-time algorithms, in terms of the number of sensors, which can be translated to distributed protocols. Habib and Safar (2007), in turn, modeled the node placement problem to improve coverage in WSNs as two sub-problems: floorplan and placement, analogous to the solution of constructing circuit boards. In this case, the considered area was first divided into well-defined geometric cells (floorplan problem), and the sensors devices had to be assigned into a set of cells (placement problem). The authors solved these two sub-problems as a single optimization problem, using an evolutionary approach to solve it. Focusing on VANETs, (Kchiche and Kamoun, 2009) proposed a greedy approach based on group centrality to select the best organization of RSUs able to provide the most stable and regular communication between vehicles. They wanted to achieve the best possible performance in terms of communication delay and overhead. Further, in (Kchiche and Kamoun, 2010), the authors showed in simulations that the use of RSUs could optimize the performance of a VANET, especially in low dense areas and in cases of long-distance communication. Moreover, (Kchiche and Kamoun, 2010) proposed strategies for RSU deployment based on centrality and equidistant, and showed that they are important factors for improving service quality.

5. Tasks of a temporary RSU

As shown in the flow diagram in Figure 2, informed vehicles that are on the boundary of coverage polygon and moving toward the scene of accident act as temporary RSUs for a certain period of time. These vehicles make a brief stop and periodically rebroadcast the safety message to mimic the role of the conventional roadside units. Vehicles that receive such message rebroadcast from these temporary RSUs follow the same procedure as shown in Figure 2. It must be noted that when one considers a different application such as instant messaging, content download, etc., the tasks of temporary RSUs may be changed - the temporary RSUs may stop for a different amount of time depending on the application; their stop duration may be preempted if the applications they support end; or instead of rebroadcasting the safety message, they may need to forward the messages to only particular vehicle(s).

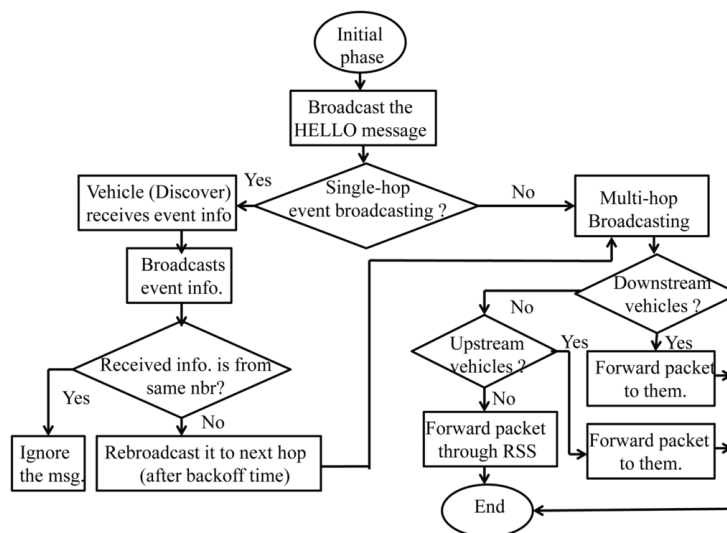


Fig. 2. A Smart Vehicular Ad Hoc Network for Efficient Data Transmission with Wireless Sensors

6. An adaptive multimedia streaming dissemination System for vehicular networks

The simulated road map is first divided into several sections, the scenario of the proposed multimedia streaming dissemination system is illustrated in Fig. 3. Based on the hierarchical framework shown in Fig. 3, a video-on-demand (VoD) streaming dissemination server collects video, and streaming data buffers are distributed at each local server. Each road section is managed by a local server, whereas an upper-level server at a higher hierarchical level is responsible for a section with a larger scope, which is composed of several nearby road sections. According to an individual user's current status, the VoD streaming dissemination server determines the amount of frames that each local server needs to prefetch and then saves data in the local server so that congestion can be effectively avoided. It is this architecture which shows the scalability of our proposed work. Notably, the VoD stream dissemination server and the local server are connected with a backbone high-speed network. Because the distance from any local server to the roadside BSs is much closer, the wired networks are used to connect the local server to the roadside BSs. Since the connections between local servers and the roadside BSs are via wired networks, and not a wireless network, a

bottleneck will not occur between local servers and the roadside BSs during the process of pre-fetching the streaming data. In this work, users are classified into two types: premium users and free users. The proposed system provides free streaming service for free users, but with limited bandwidth. In the case of a shortage of the bandwidth, the quality of the streaming data, compression ratio, and frame per second (fps) for the free users will be degraded in order to release more bandwidth to meet the minimum bandwidth requirements for the premium users who have higher priority. Accordingly, the free users cannot only obtain free seamless streaming service, but they also help premium users to keep accessing Internet resources without interruption and degradation of the service. Hence, a win-win situation could be achieved in our proposed scheme. When a vehicle enters the coverage of a roadside BS, the streaming data will be forwarded to the vehicle via the roadside BS, as illustrated by the V2I symbol in Fig. 3.

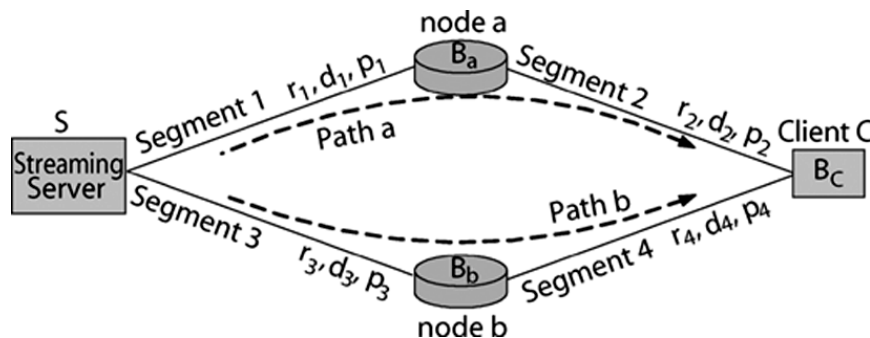


Fig.3. Typical multipath streaming scenario

7. Conclusion

Based on the designed local rules, a DSRC-equipped vehicle independently determines whether it should serve as an RSU; and if so, it stops for a small duration and rebroadcasts the message. Results show substantial improvement in terms of message reachability which is crucial for safety message dissemination application in VANETs. While the solution proposed to the RSU deployment problem is interesting in itself, perhaps even a more interesting global conclusion is how the biologically inspired approach to solving fundamental transportation problems can be generalized and used as a powerful approach and tool for solving several important transportation problems. Our ongoing work is currently looking into other instances of the same approach for solving other outstanding transportation problems.

REFERENCES

- Hartenstein et al. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 46(6):164–171.
- Li and Wang. (2007). Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, 2(2):12–22.
- Yousefi et al. (2006). Vehicular ad hoc networks (VANETs): Challenges and perspectives. In 6th International Conference on ITS Telecommunications Proceedings, pages 761–766, Chengdu, China.

Toor et al. (2008). Vehicle ad hoc networks: applications and related technical issues. *IEEE Communications Surveys & Tutorials*, 10(3):74–88.

Bakhouya et al. (2011). An adaptive approach for information dissemination in vehicular ad hoc networks. *Journal of Network and Computer Applications*, 34(6):1971–1978.

Lochert et al. (2009). Information dissemination in VANETs. In *VANET: Vehicular Applications and Inter-Networking Technologies*, chapter 3. John Wiley & Sons Ltd., Chichester, UK.

Toutouh and Alba. (2011). An efficient routing protocol for green communications in vehicular ad-hoc networks. In *13th annual conference companion on Genetic and evolutionary computation*, Dublin, Ireland.

Trullols et al. (2010). Planning roadside infrastructure for information dissemination in intelligent transportation systems. *Computer Communications*, 33(4):432 – 442.

Macedo et al. (2012). (CIA) 2-ITS: Interconnecting mobile and ubiquitous devices for intelligent transportation systems. In *IEEE Pervasive Computing and Communication*, Lugano, Switzerland.

Filippini et al. (2012). Non-cooperative rsu deployment in vehicular networks. In *9th Annual Conference on Wireless On-demand Network Systems and Services*, pages 79–82. IEEE.

Habib and Safar. (2007). Sensitivity study of sensors' coverage within wireless sensor networks. In *Proceedings of 16th International Conference on Computer Communications and Networks*, pages 876–881.

Kchiche and Kamoun. (2009). Access-points deployment for vehicular networks based on group centrality. In *3rd International Conference on New Technologies, Mobility and Security*, pages 207–2012, Cairo, Egypt.

Kchiche and Kamoun. (2010). Centrality-based access-points deployment for vehicular networks. In *17th International Conference on Telecommunications (ICT)*, pages 700–706, IEEE.

Impact of sink node position in the human body on the performance of WBAN

Raju sharma¹, Hardeep Singh Ryait², Anuj Kumar Gupta

¹ Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India

*² Professor, Department of Electronics and Communication Engineering
Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India*

*³ Professor, Department of Computer Science and Engineering
Chandigarh Engineering College, Mohali, Punjab, India*

Abstract- *Wireless* body area networks consisting of various sensor nodes which are deployed on or in the human body to sense the vital sign of the human body. It is used to improve the QoS of life, healthcare applications and remote patient monitoring. Sensor nodes are placed on the human body; they sense the signal and send it to sink. Due to the movement of the body parts distance between the sensor node and sink increased or decreased which affect the performance of the network. In these networks routing protocols plays an important role together with position of sink node. Previous research shows that the best position to place the sink node in the human body is the center of the human body (waist). This paper analyzes the performance of routing protocol with arm movement by placing sink node at waist and compare these results with the results when the sink node is placed at the center of the network. Parameters used to compare the results are Stability period, Network lifetime, and Packet drop. Results show that stability and network lifetime is increased when the sink node is placed at center of network.

I. INTRODUCTION

A wireless Body area network is a collection of small size, intelligent, light weighted sensor nodes which are placed in or on the human body. These sensors nodes are used to sense, process and transmit the vital sign of the human body to the sink node. Doctors can then access the data collected by the sink node and do the treatment according to the requirement. This gives the patients flexibility to move liberatingly by liberating from the requirement to be connected to the hospital equipment to monitor their conditions [1]. This additionally obviates patient from any kind of sudden attack. According to application point of view WBAN can be divided into two parts[4].

1.1 Medical WBAN

In Medical WBAN implant and wearable sensor nodes are acclimated to quantify the health status of the human body. Medical WBAN can be relegated as: (a) Wearable WBAN and (b) implantable WBAN.

1.2 Non-Medical WBAN.

Wearable consumer electronics and regalement contrivances are the examples of Non-Medical WBAN.

1.3 Mainly three types of nodes used in WBAN [1]

1. Implant node: Implantable nodes are those nodes which are placed inside the human body just below the skin.
2. Body Surface node: Body surface node is those nodes which are placed on the surface of the human skin.
3. External node (Gateway Node): External nodes do not have any contact with the human skin.

II. MOTIVATION

In SIMPLE protocol [2] 8 sensor nodes are placed on the human body at fine-tune position to quantify the vital denotement of the human body. There are withal two types of communication models are utilized direct and multi-hop communication. Consequential data is transmitted directly to the sink on the other hand mundane data is transmitted to the sink through forwarder node. Forwarder node is culled utilizing a cost function. Cost function depends on two parameters distance and residual energy of the sink. if the residual energy of the sensor node is less than the threshold level sensor nodes uses direct communication to send data to sink.

In WBAN sensor nodes are deployed on the human body, there is node mobility present due t body parts movement and network topology also varies due to node mobility[3]. The radio connection between the nodes and the channel quality depends on the relative position of sensor nodes with respect to sink. Mobility model have a big impact on the performance of simulations for WBAN. Simulating a protocol for WBANs without considering the mobility of body parts is not reliable at all [5]. In this paper we analyze the performance of the simple protocol under arm movement when the sink is placed at the waist of the human body. This work check the impact of body parts mobility on the performance of the SIMPLE routing protocol and compare the results that are obtained when the sink node is placed at center of the network.

III. SYSTEM MODEL AND PROPOSED TECHNIQUE

Performance analysis of SIMPLE protocol with sink node placement strategy

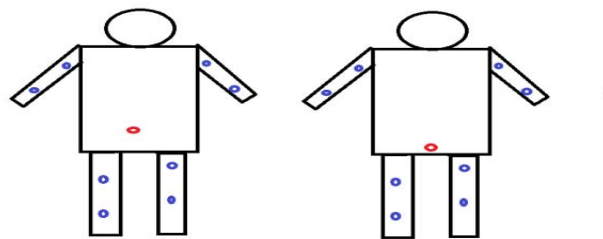


Figure .1: (a) Sensor nodes and sink node placement in the human body.

8 sensor nodes are placed in the human body as shown in Figure 1. performance is evaluated by placing the sink node at two different positions. First position of the sink is the waist center of the human body (CTH) and the second position of the sink is center of the network (CTN) which is formed by the sensor nodes which are placed on the human body. X and Y coordinates or the sensor nodes are shown below

$$X_m = 2.0$$

$$Y_m = 0.8$$

$$Se(i).xd = [0.2, 0.6, 0.7, 0.5, 0.1, 0.35, 0.5, 0.35] \quad (1)$$

$$Se(i).yd = [1.2, 1.1, 0.8, 0.6, 0.8, 0.5, 0.3, 0.1] \quad (2)$$

No of sensor nodes=8

When the sink node is placed at the center of the human body .it is placed at

Sink.x=0.4

Sink.y=1

In second case when sink is placed at the center of the network.In this case average is calculated by adding the the x y coordinates of all the nodes

$\text{Sink.x} = \frac{\text{Se}(1).\text{xd} + \text{Se}(2).\text{xd} + \text{Se}(3).\text{xd} + \text{Se}(4).\text{xd} + \text{Se}(5).\text{xd} + \text{Se}(6).\text{xd} + \text{Se}(7).\text{xd} + \text{Se}(8).\text{xd}}{n};$

$\text{Sink.y} = \frac{\text{Se}(1).\text{yd} + \text{Se}(2).\text{yd} + \text{Se}(3).\text{yd} + \text{Se}(4).\text{yd} + \text{Se}(5).\text{yd} + \text{Se}(6).\text{yd} + \text{Se}(7).\text{yd} + \text{Se}(8).\text{yd}}{n};$

sink.x=0.41

sink.y=0.67

IV. RESULTS AND DISCUSSION

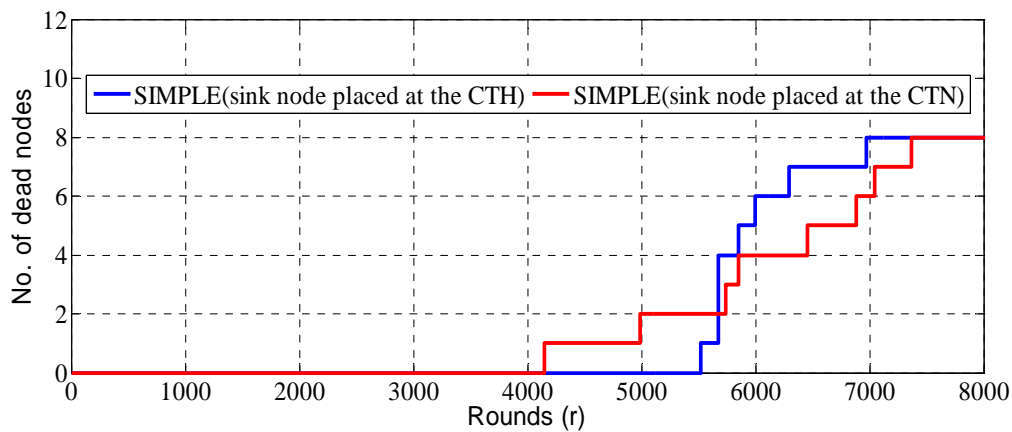


Figure 2 .Stability and Network lifetime Analysis

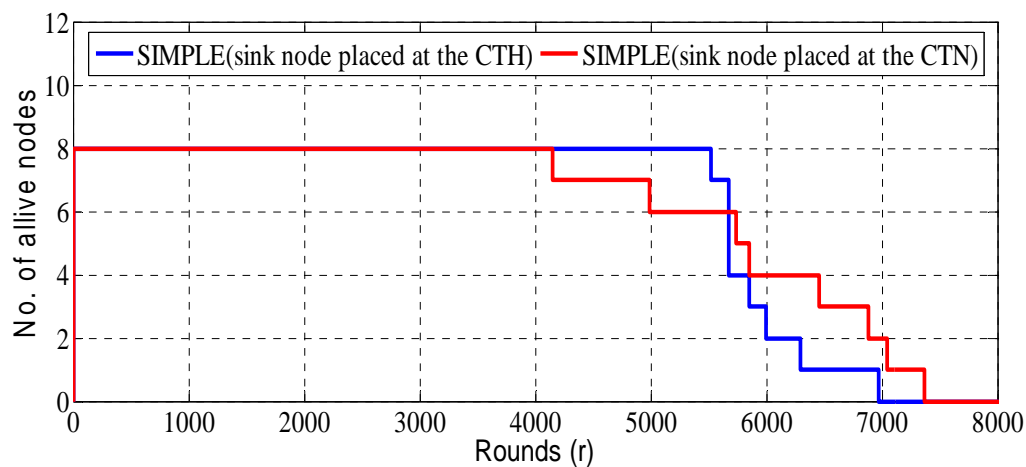


Figure 3. No of alive nodes

Figure 2. shows the comparison of network lifetime when the sink node is placed at waist of the human body (blue line) and center of the network (red line). When the sink node is placed at waist of the human body first node dead at 5500 Rounds and in case of 2nd position 1st node dead at 4200 Rounds. According to first node dead 1st position of sink provides more stability than 2nd position. But at 6000 Rounds there are 6 nodes dead at 1st position and only 4 nodes dead at 2nd position. At 7000 Rounds all the sensor nodes are dead at 1st position and in 2nd position all nodes are dead at 7300 Rounds. From the results it is concluded that overall network is more stable and have longer lifetime when the sink node is placed at the center of the network. Figure 2. also shows that the nodes alive for longer duration when the sink node is placed at the center of the network .

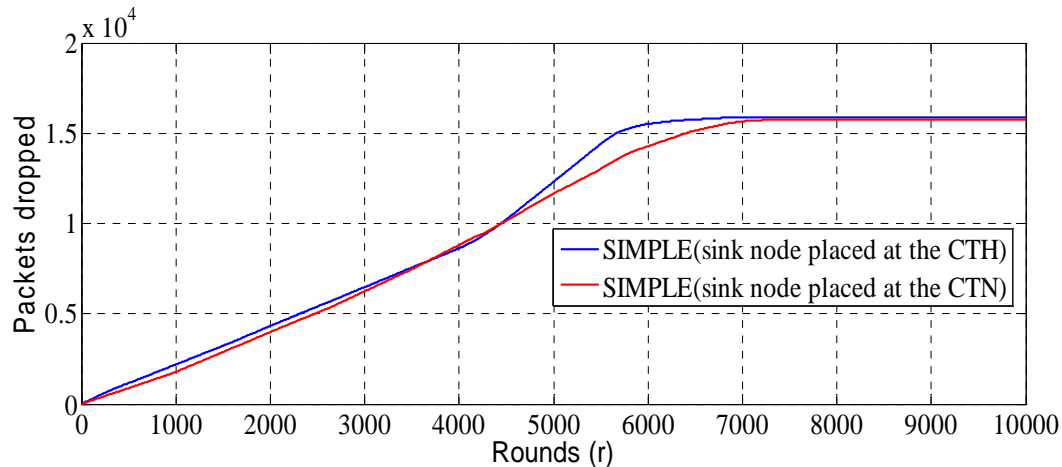


Figure 4. Packet dropped

For the calculations of dropped packets uniformed model is used. In this model status of the link is compared with the desired level which is responsible for successful transmission of packets. If the status of the link is below the required level packet dropped. Figure 4. shows that more packets dropped when the sink is placed at the center of the human body.

V. ARM MOVEMENT

Performance analysis of SIMPLE protocol with Arm movement sink node placement strategy

Figure 5. shows the position of sensor nodes and sink node under arm movement. Two arm positions are shown in the following Figure.

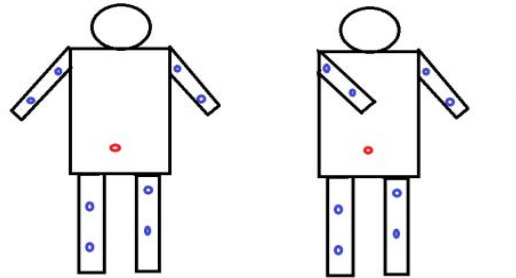


Figure 5. Arm movement when sink node placed at the waist of the human body (CTH)

Table 1.Distance of sensor nodes from sink nodes under two positions of the sink nodes with arm movement.

	Position1	Position 2	Position 1	Position 2
Nodes	Sink placed at waist		Sink placed at CTH	
1	0.3606	0.3606	0.5701	0.5701
2	0.2828	0.2828	0.4701	0.4701
3	0.3162	0.3162	0.3178	0.3178
4	0.3162	0.3162	0.1140	0.1140
5	0.3162	0.1414	0.3362	0.3421
6	0.4031	0.4031	0.1803	0.1803
7	0.6083	0.6083	0.3808	0.3808
8	0.8016	0.8016	0.5731	0.5731
Sink placed at	0.4	0.4	0.41	0.41
	0.9	0.9	0.67	0.67

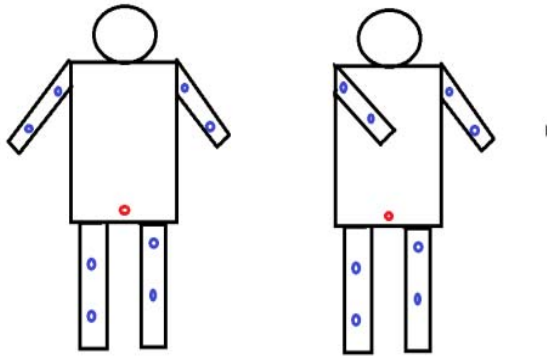


Figure 6. Arm movement when sink is placed at the center of the network (CTN)

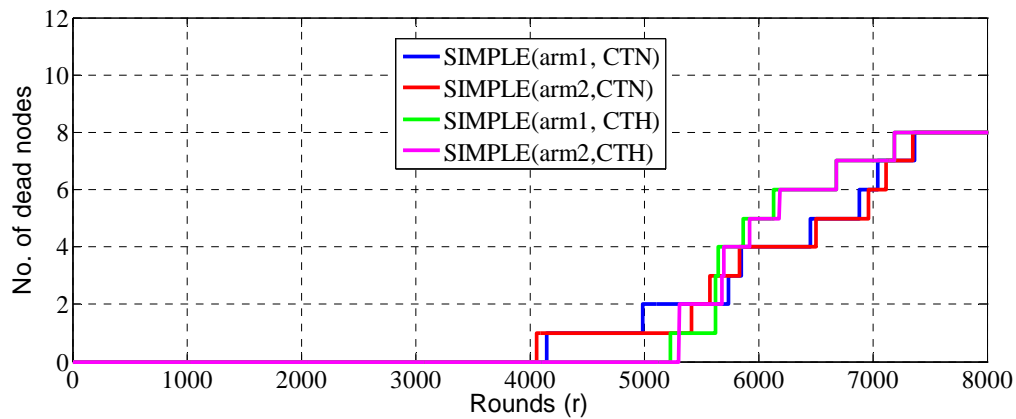


Figure 7. Network lifetime analysis

Fig show the comparison of two sink node locations along with arm movement. It is clear from the results that the network lifetime is increased when the sink node is placed at the center of the network with arm movement. Fig(5) shows that the sensor nodes are alive for more time in CTN than CTH.

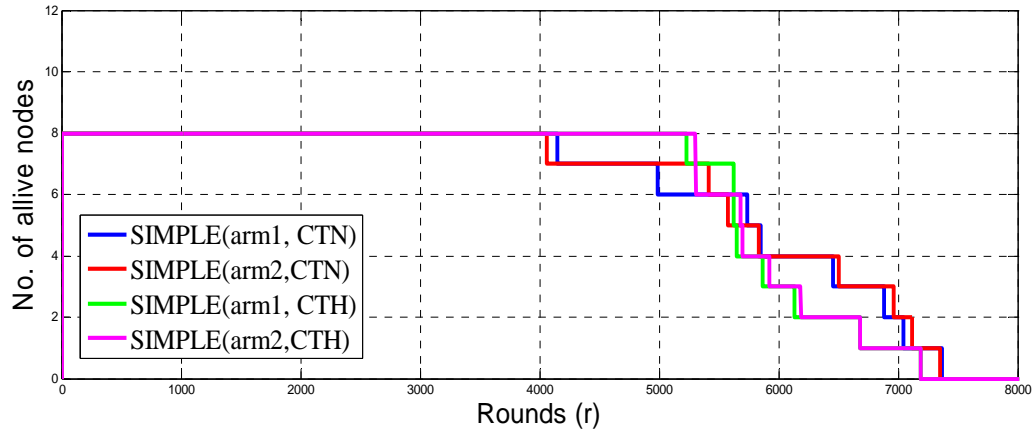


Figure 8. No of alive nodes

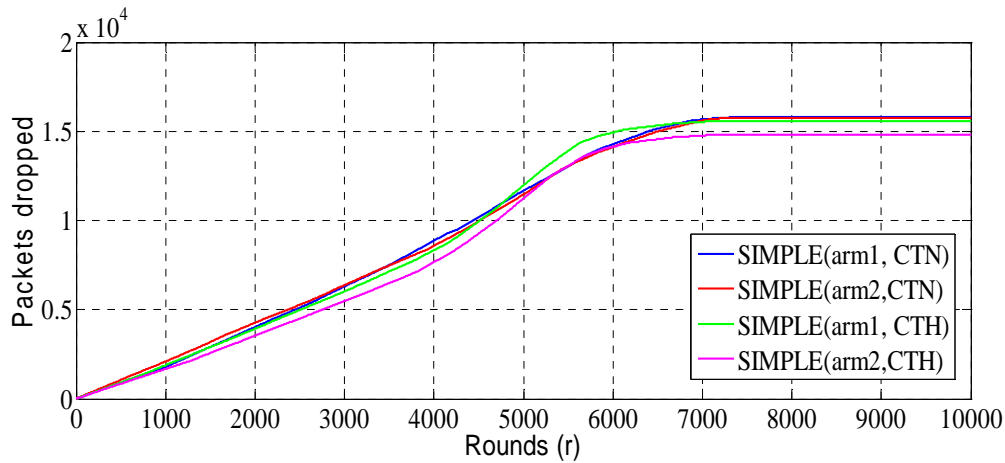


Figure 9.No of packet dropped

Figure.9 Shows that more packets are dropped in first position of arm when sink node is PLACED at CTN and 2nd position of arm when the sink node is placed at CTH.

VI. CONCLUSION

This paper mainly deals with the placement of the sink node in the human body. Two sink node positions are analyzed in this paper one is the center of the human body and the second is the center of the network. In first scenario it is concluded that the network lifetime is more when the sink is placed at CTN. In second scenario arm mobility is considered along with sink placement. From this it is also clear that network lifetime is more at CTN. From the complete analysis it is find that he best position to place the sink in human body is the center of the network.

REFERENCES

- [1] K. Y. Yazdandoost and K. Sayrafian-Pour, "Channel Model for Body Area Network(BAN)", IEEE802.15.6 technical contribution, document ID: 15-08-0780-09-0006, 27 April, 2009, pp. 41-56.
- [2] Nadeem, Q. Javaid, N. ; Mohammad, S.N. ; Khan, M.Y. ; Sarfraz, S. ; Gull, M., "SIMPLE: Stable Increased-Throughput Multi-hop Protocol for Link Efficiency in Wireless Body Area Networks", Published in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, 28-30 Oct. 2013, pages. 221 – 226.
- [3] Md Tanvir Ishtaique-ul Huque, Kumudu S. Munasinghe, "Body Node Coordinator Placement Algorithms for Wireless Body Area Networks", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 1, FEBRUARY 2015.
- [4] Luis Filipe, Florentino Fdez-Riverola, Nuno Costa, and António Pereira "Wireless Body Area Networks for Healthcare Applications: Protocol Stack Review", International Journal of Distributed Sensor Networks Volume 2015 (2015), Article ID 213705, 23 pages
<http://dx.doi.org/10.1155/2015/213705>
- [5] Anum Talpur ,Natasha Baloch,Nafeesa Bohra,Faisal Karim Shaikh ,Emad Felemban, "Analyzing the Impact of Body Postures and Power on Communication in WBAN", Procedia Computer Science Volume 32, 2014, Pages 894–899

Formal Concept Analysis to Improve Robustness on Medical Image Watermarking Schemes in the Spatial Domain

Muath AlShaikh

Lab-STICC (UMR CNRS 6285), University of Western
Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS
93837, 29238 Brest Cedex, France

Lamri Laouamer

Department of Management Information Systems, CBE,
Qassim University P.O. Box 6633, Buraidah, 51452, KSA

Laurent Nana

Lab-STICC (UMR CNRS 6285), University of Western
Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS
93837, 29238 Brest Cedex, France

Anca Christine

Lab-STICC (UMR CNRS 6285), University of Western
Brittany, Brest, 20 avenue Victor Le Gorgeu, BP 817 - CS
93837, 29238 Brest Cedex, France

Abstract — Digital medical image plays an important role in the field of Telemedicine, but patient privacy and other security issues are still coming under threats from unauthorized users. Watermarking has become essential and required for proving the identity of the owner, as well as authorizing use of images and also protecting copyrighted material from illegal access. Authorizing use and copyright protection as parameters of an image, especially of a medical image, are strongly related to robustness and complexity, imperceptibility and capacity as parameters of watermarking. Medical images have a special structure which comprises header and body blocks. The region of non interest (NROI) in the body of a medical image is the most suitable area for embedding watermark to prevent the degradation of the medical image. In our paper, we propose a novel watermarking approach in the spatial domain, based on formal concept analysis (FCA). FCA finds the optimal position for watermark embedding in NROI of the medical image. Our watermark is built from some existing information in the DICOM header (IODs). Experimental results indicate that the proposed approach would offer us high robustness with less complexity, imperceptible embedding and low payload compared with the existing watermarking approaches.

Keywords- FCA; Watermarking; Spatial Domain; Attacks; Robustness.

I. INTRODUCTION

With the huge development and the rapid growth in information technology and communication tools, the internet has become the main communication channel for transmitting, sharing and exchanging the data between users. Moreover, digital medical images are considered as the main aim for Telemedicine and Telesurgery treatments and diagnoses and the physician makes the diagnosis based on medical image content. However, this popularity introduces a new challenging problem with regard to security issues such as copyright infringement and proof of ownership. To address these issues, we need to enhance the techniques that can protect digital materials against intentional and unintentional attacks, through

high robustness and low computational complexity [1, 2]. Indeed, some of these attacks may be detected using an ownership or copyright proof. If we consider, for example an attack consisting in modifying the source image by substitution, the absence of the right information on ownership or copyright make it possible to detect the attack.

Telemedicine consists of the use of information and communications techniques to offer the healthcare where patients and physicians are separated by physical distance. Modern healthcare systems, such as Hospital Information System (HIS) and Picture Archiving and Communication System (PACS), provide the health sector with the digital medical information in ways that are both rapid and easy. This huge quantity of data needs to be stored, processed and managed with regard to security and safety issues like confidentiality and reliability, which involves integrity and authentication. Figure 1 shows a diagrammatic schema of Telemedicine [3, 4].



Figure 1. Diagrammatic Schema of Telemedicine

Recently, digital watermarking has been considered as a solution for earlier such problems, since the watermark can prove the identity of the authorized owner of the images. Digital watermarking consists of two parts; one part that

consists of embedding the watermark in the host image. The second part consists of the watermark extraction [5].

Cryptography is another method to protect the digital material. It makes it possible to send the data in a secure format. Only the authorized user can decode and read it. The data is protected during the transmission since it is in encrypted form. But after the decryption process, the data are no longer protected. So, the data is easy to modify, tamper or rob. This aspect is the main shortcoming of the cryptographic techniques, while the watermarking techniques have the ability to cover these protection issues [6]. Moreover, according to the complexity, the most known of the cryptography approaches requires a high complexity [7].

To fulfil the requirements of watermarking, we have to prove that it has the following characteristics: a) robustness, which depends on the capacity of watermark to resist different kinds of attacks; b) imperceptibility: the watermark does not affect image quality and is invisible to human eyes; and c) the capacity of the method, which considers the numbers of bits that are used for watermark embedding. There is a trade-off between these requirements. Moreover, complexity is also important for embedding and extraction techniques: because we work in real-time environments [8, 9]. Figure 2 illustrates the tradeoffs that exist among watermarking characteristics and requirements.



Figure 2. Trade-offs among watermarking requirements

Watermarking technique domains are classified into two categories: spatial and frequency. In the spatial domain, the watermarks are embedded directly into the material, as with the Least Significant Bit (LSB) method. This is simple and fast, but has a low robustness against attacks [10, 11]. In the frequency domain, watermarks are embedded into coefficients of frequency transform of the material, like Discrete Wavelet Transform DWT and Discrete Cosine Transform DCT. The techniques in frequency domain are high in robustness, high in capacity and complexity terms compared with the techniques in the spatial domain[12, 14].

Digital medical imaging and communication in medicine (DICOM) describes the data structure of a medical image; it is made up of two parts: header and body. The header covers Information Object Definitions (IODs), which contain the patient information (name, age, date of birth, etc.), hospital information, physician information and other details. The body part includes the region of interest (ROI), which contains the

most important information which serves for physicians' diagnoses. Any modifying in this part will affect the images. The DICOM format has also the region of non interest (NROI), which is normally at the edge and the background of the image. Embedding the watermark in the NROI would avoid any modification of the medical images and degradation in term of quality [11, 13, 14].

This paper presents a novel robust approach for medical image watermarking in the spatial domain, based on the Formal Concepts Analysis FCA model. The FCA allows us to determinate an optimal insertion position in the non-region of interest (NROI) of medical images. We extract the watermark from the header of medical image information (IODs) defined by Patient Name, Patient Date Of Birth, Patient Age and File Modified Date information. There are relations between these types of watermark information that can help us to know if any (cutting, adding, replacing) attacks have happened (Tamper Detection). Our experimental results show that we extract the embedded watermark image with high quality, low payload and low computational complexity from the attacked watermarked image after attack scenarios.

II. FORMAL CONCEPT ANALYSIS (FCA)

FCA was initially developed in data analysis, knowledge representation and knowledge discovery in databases (KDD) [15]. The FCA can provide support for processing large dynamic, complex data sets with additional knowledge. It is a sub field of applied mathematics based on the lattice theory. Starting from a formal context built by a set of objects that share a number of properties, this method returns a lattice with a special property, the Galois property. The objects, and the properties which are also called attributes, can be more or less abstract depending on the type of application. In different applications, the appropriate choice of the context allows to obtain more information from the this lattice. The FCA has been applied in various fields such as data mining, conceptual modelling, social networks and the semantic web [15, 16]. For FCA in ontology engineering, [17] was the first paper using FCA in combination with ripple-down rules to extract ontological vocabulary from knowledge bases. FCA played the role of a tool for ripple down rules (RDR), performing the derivation of concepts and the relation between them. The authors in [18] combined FCA with natural language processing for building an ontology in the field of cardiovascular medicine. In our paper, this theory is applied with an appropriate choice of objects and attributes in order to determine the region of encryption of the watermark. Let us do a short presentation of the FCA.

A. FCA Definition

The basic notions in FCA are: a formal context that is a triple set $B(G, M, I)$, where $I \subseteq G \times M$ is a binary relation. This triple set can be represented by a cross table, as a set of rows G (formal objects) and a set of columns M (formal attributes);

the points where they cross represent the relation I. The notation gIm stands for $(g, m) \in I$, which is read as: the object g has the attribute m [19].

Two sets X' and Y' are defined :

For X a subset of attributes, $X' = \{g \in G | gIm \text{ for all } m \in X\}$ (1)
the set of all objects in G sharing all attributes in X

For Y a subset of objects, $Y' = \{m \in M | gIm \text{ for all } g \in Y\}$ (2)
the set of all attributes in M falling under all objects in Y

A formal concept is considered to be a unit of two parts: the Extent (a set of objects), and the Intent (a set of attributes) such that all the objects in Extent have all the attributes in Intent and conversely i.e. all the attributes in the Intent fall under all objects in Extent.

B. Sub-concept relation, Super-concept relation Maintaining the Integrity of the Specifications

The concept $(A1, B1)$ is a sub-concept of the concept $(A2, B2)$ if $A1 \subseteq A2$ or $B2 \subseteq B1$. So $(A2, B2)$ is a super-concept of $(A1, B1)$. The relation sub-concept–super-concept is denoted by \leq . Being a sub-concept of a super-concept means that the extension of the sub-concept is contained in the extension of the super-concept, which is equivalent to the relationship where the intention of the super concept contains the intention of the sub-concept [20].

FCA can be illustrated more clearly through an example. Let us suppose we have records for a set of images. For each image, there is a set of its features. We note the features (M) , $M = \{1, \dots, 8\}$, as shown in

TABLE I. THE IMAGES AND THEIR FEATURES

Features	Description
1	Grayscale
2	Color
3	Smooth
4	Nature
5	Flat
6	Attacked
7	Watermarked
8	YCbCr

TABLE II. FORMAL CONCEPTS OF DATA GIVEN BY THE IMAGES AND THEIR FEATURES

C_i	$\langle A_i, B_i \rangle$
C0	$\langle \{\}, \{1, 2, 3, 4, 5, 6, 7, 8\} \rangle$
C1	$\langle \{1, 5, 9, 11\}, \{1, 2, 3, 5\} \rangle$
C2	$\langle \{2, 4, 12\}, \{1, 2, 6, 8\} \rangle$
C3	$\langle \{3, 6, 7\}, \{2, 5, 7\} \rangle$
C4	$\langle \{3, 6, 7, 8, 10\}, \{7\} \rangle$
C5	$\langle \{1, 3, 5, 6, 7, 9, 11\}, \{2, 5\} \rangle$
C6	$\langle \{1, 2, 4, 5, 9, 11, 12\}, \{1, 2\} \rangle$
C7	$\langle \{1, 2, 3, 4, 5, 6, 7, 9, 11, 12\}, \{2\} \rangle$
C8	$\langle \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, \{\} \rangle$

In table 1, we have 12 images (G) , $G = \{1, \dots, 12\}$. Our example describes the images and their features in 12×8

binary matrix I (Table 2). In the following, C refers to a concept, and A and B are extent and intent, respectively.

In table 2, the first formal concept, $C0$, contains zero object (extent) with all attributes (intent), which means no image contained all the descriptions. For the second formal concept, $C1$, the images 1, 5, 9 and 11 contain features 1,2,3,5. In the last concept, $C8$, it means that there is no image that contained all the features. The first concept includes zero object with all attributes and the next concept includes the sharing objects with their attributes and so on to the last concept. We denote the extent is increasing and the intent is decreasing until the intent is empty intent= \emptyset (Incrementing way). In the same way, if we take a look at the concepts from $C0$ to $C8$, we note that the concept $C8$ includes all its extent (objects) with empty intent (attributes) and that the next concept decreases the extent and increases the intent until the extent becomes the empty set extent= \emptyset (Decrementing way). Figure 3 illustrates the lattice called also formal concept analysis line diagram between the images and the features they contain.

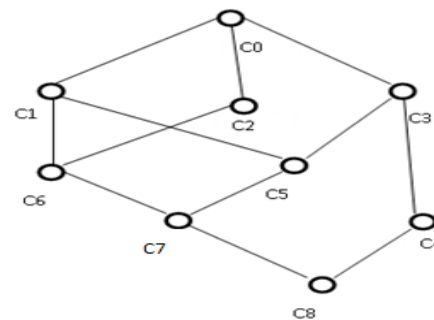


Figure 3. Line diagram of formal concept analysis for images and their features

We apply the FCA principle in the watermarking techniques to determine the optimal position of embedding, in order to obtain low complexity, low capacity, high robustness and high imperceptibility for the embedding and the extraction process.

III. THE PROPOSED APPROACH

A. Embedding Phase

Figure 4 illustrates the watermark embedding scheme. Our embedding steps can be summarized by the following:

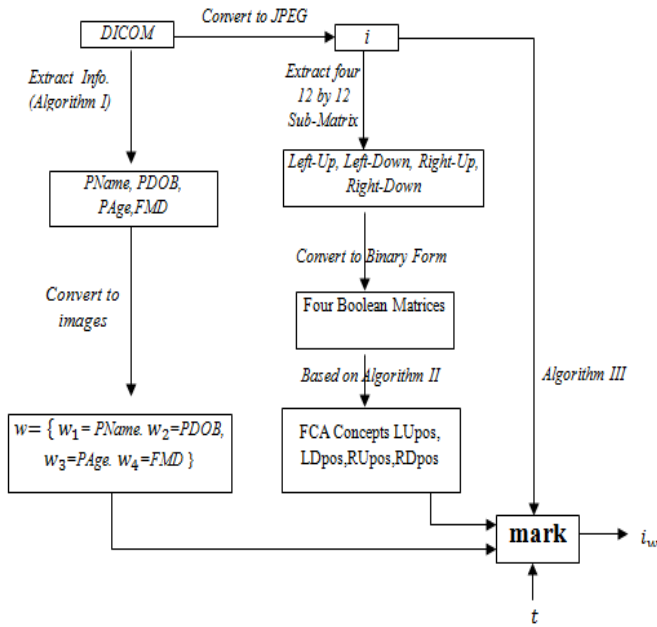


Figure 4. Watermark embedding scheme

1) We generate out the watermark information from the header of the medical image. The watermark information includes the Patient Name (PName): first watermark (w_1), Patient Date Of Birth (PDOB): second watermark (w_2), Patient Age (PAge): third watermark (w_3), and File Modified Date (FMD): fourth watermark (w_4), as illustrated in the algorithm I. We have chosen these four watermark information from IOD's because there is a relation between them and, then, we can verify if the relation is kept. In our approach we calculated, from FMD and PDOB, the age and we compared the result with the watermark age.

$$w = \{w_1, w_2, w_3, w_4\} \in \text{IODs}$$

The building of the watermark from the DICOM header can be summarized as follows:

Algorithm I

INPUT: DICOM Image

OUTPUT: w_1, w_2, w_3, w_4 (watermarks) // as four JPEG images

Read DICOM image

Extract the PName, PDOB, PAge and FMD

$w_1 \leftarrow$ JPEG conversion of PName.

$w_2 \leftarrow$ JPEG conversion of PDOB.

$w_3 \leftarrow$ JPEG conversion of PAge.

$w_4 \leftarrow$ JPEG conversion of FMD.

end

2) We isolated the zero area and started the extraction from the data area in NROI. We extracted a four 12×12 sub-matrices from the original image i : Left-Up, Left-Down, Right-Up, Right-Down, as we can see in figure 5. Then, we converted the pixel values to the binary form and the result

gave us a four 144×8 Boolean matrices, as we can see in figure 6.

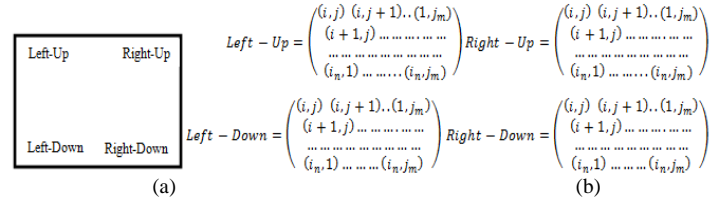


Figure 5. (a) Extraction of four 12×12 sub-matrices from i , (b) Decimal representation of each sub-matrix

$$\begin{aligned} \text{Left-Up} &= \begin{pmatrix} 00000001 \\ \dots \\ 00001001 \end{pmatrix} & \text{Right-Up} &= \begin{pmatrix} 00010101 \\ \dots \\ 00001100 \end{pmatrix} \\ \text{Left-Down} &= \begin{pmatrix} 00001000 \\ \dots \\ 00000100 \end{pmatrix} & \text{Right-Down} &= \begin{pmatrix} 00001001 \\ \dots \\ 00010100 \end{pmatrix} \end{aligned}$$

Figure 6. 144×8 Boolean Matrix for each area picked up

3) We built the FCA concepts for Left-Up, Left-Down, Right-Up, Right-Down Boolean matrices. All the process of transformation of matrices Left-Up, Left-Down, Right-Up, Right-Down to obtain their FCA concepts is given by Algorithm II.

Matrices LUcon, LDcon, RUcon, RDcon. Here below contain all formal concepts built by FCA for Left-Up, Left-Down, Right-Up, Right-Down. The first group represents the extent and the second represents the intent. Because of the length of the concepts we could not list all elements of their extent and intent:

$$\text{LUcon} = \langle \{133, 160, 176, \dots\}, \{9, 10, 11, 12, \dots\} \rangle, \langle \dots \rangle \quad (3)$$

$$\text{LDcon} = \langle \{403, 412, 43, \dots\}, \{12, 15, 17, 21, \dots\} \rangle, \langle \dots \rangle \quad (4)$$

$$\text{RUcon} = \langle \{133, 137, 152, \dots\}, \{494, 498, 500, \dots\} \rangle, \langle \dots \rangle \quad (5)$$

$$\text{RDcon} = \langle \{399, 442, 446, \dots\}, \{496, 499, 500, \dots\} \rangle, \langle \dots \rangle \quad (6)$$

4) We built the FCA matrix positions for each region. The matrix position is a matrix built based on the extent (A) and the intent (B) as pair (A, B) of coordinates for each concept (elements of the sets extent \times intent).

The extraction of the four regions of i , the building of the FCA lattice and the generation of the FCA matrix for each region are done as follows:

matrix for each region are done as follows:

Algorithm II

INPUT: i (Original image)

OUTPUT: positions(LU, LD, RU, RD) // positions obtained from FCA, which are used for embedding

// To extract the four regions of the original image leftUp, leftDown, rightUp, rightDown


```

// Find the FCA concepts for each region, where A is extent
and B is intent
    con1 = concepts(leftUp)// n1 is the number of the
concepts in LU
    con2 = concepts (leftDown)// n2 is the number of the
concepts in LD
    con3 = concepts (rightUp)// n3 is the number of the
concepts in RU
    con4 = concepts (rightDown)// n4 is the number of the
concepts in RD
//Build position matrix from FCA concepts
for i = {1,2,3,4}
    posi = {}
    for each e in coni
        posi ← posi ∪ e(1) * e(2)
    end
end
position = (pos1, pos2, pos3, pos4)
function concepts
INPUT: Region// leftUp, leftDown, rightUp, rightDown
OUTPUT : SetOfConcepts
// Initialize the concept list to empty set.
SetOfConcepts = {}
//Convert the region into binary matrix
BinMat = dec2bin(region,8)
    for each row G in BinMat
        for each column M in BinMat
            if BinMat(G, M)
                for each column S in BinMat
                    if BinMat(G, S)
                        add the column number to B
                        for each column S1 in B, and each
row G1 in BinMat
                            if BinMat(G1, S1)
                                add the row number to A
                        end
                    end
                add (A,B) to SetOfConcepts
            end
        end
    for each item in (Ai,Bi) replace the value with zero
in BinMat
        B = {} and A = {};
    end
    return SetOfConcepts.
end

```

5- We embedded the four watermarks in the four regions Left-Up, Left-Down, Right-Up, Right-Down of the original image, as illustrated in algorithm III, by using the following linear interpolation:

$$iw = \{iw_{LU}, iw_{LD}, iw_{RU}, iw_{RD}\} \quad (7)$$

$$iw_{LU} = (1 - t)w_1 + t iw_{LU} \quad (8)$$

$$iw_{LD} = (1 - t)w_2 + t iw_{LD} \quad (9)$$

$$iw_{RU} = (1 - t)w_3 + t iw_{RU} \quad (10)$$

$$iw_{RD} = (1 - t)w_4 + t iw_{RD} \quad (11)$$

Where $t \in]0,1[$ such that iw , w_1 , w_2 , w_3 and w_4 are the watermarked image and the four watermark images, iw_{LU} , iw_{LD} , iw_{RU} , iw_{RD} respectively, representing the Left-Up, Left-Down, Right-Up and Right-Down positions in the watermarked image. Here, iw_{LU} , iw_{LD} , iw_{RU} , iw_{RD} represent Left-Up, Left-Down, Right-Up and Right-Down positions in the original image. The position we use is that extracted based on FCA from the Boolean matrices.

The embedding steps can be summarized as the following algorithm (algorithm III):

The embedding steps can be summarized as the following algorithm (algorithm III):

Algorithm III

INPUT: i (original image), four watermark images (w_1, w_2, w_3, w_4), positions

OUTPUT: iw (watermarked image)

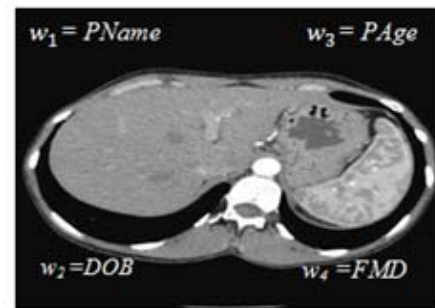
```

for each item in  $w_1$  watermark
     $iw(\text{positions}(LU)) = (1-t)*w_1 + t*iw(\text{positions}(LU))$ 
for each item in  $w_2$  watermark
     $iw(\text{positions}(LD)) = (1-t)*w_2 + t*iw(\text{positions}(LD))$ 
for each item in  $w_3$  watermark
     $iw(\text{positions}(RU)) = (1-t)*w_3 + t*iw(\text{positions}(RU))$ 
for each item in  $w_4$  watermark
     $iw(\text{positions}(RD)) = (1-t)*w_4 + t*iw(\text{positions}(RD))$ 

```

Save iw Image

Figure 7 illustrates the watermarked image after embedding the four watermark images (w_1 , w_2 , w_3 , w_4) by using the linear interpolations in four regions (Left-Up, Left-Down, Right-Up, Right-Down), based on FCA concepts, to determine the positions in the NROI of original image i .



A			
Muna	10/10/86	29Y	2/1/15
(a)	(b)	(c)	(d)
B			

Figure 7. iw and w : watermarked and watermark images

A watermarked image

B a) pname watermark, b) dob watermark, c) page watermark, d) fmd watermark

Figure 7 B represents our watermark image, which includes information extracted from the DICOM header IODs; each watermark is converted into an image.

We used the original image in 512×512 sizes. Figure 8 illustrates the original image and the watermarked images for two different values of factor t . As we can see in this figure, when t is close to 1 the watermark is invisible and no degradation in the image quality (figure 8, (b)), but if the t is close to 0 the watermark is visible and there is a little degradation in the image quality, as we can see in figure 8, (c).

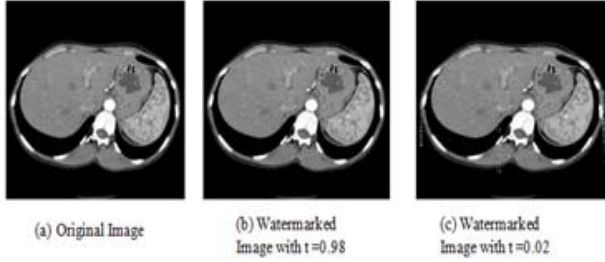


Figure 8. Watermark embedding with different values of t : (a) Original image, (b) and (c) watermarked images

B. Extraction phase

In the extraction phase (algorithm IV), the matrix positions that are extracted from a Boolean matrix based on FCA are required (LUpos, LDpos, RUpos, RDpos). Then the extraction done by using the linear interpolations is as follows:

$$W_{a1} = \frac{1}{t} W_1 - \frac{1-t}{t} i_{wa1LUpos} \quad (12)$$

$$W_{a2} = \frac{1}{t} W_2 - \frac{1-t}{t} i_{wa2LDpos} \quad (13)$$

$$W_{a3} = \frac{1}{t} W_3 - \frac{1-t}{t} i_{wa3RUpos} \quad (14)$$

$$W_{a4} = \frac{1}{t} W_4 - \frac{1-t}{t} i_{wa4RDpos} \quad (15)$$

Such that w_{a1} , w_{a2} , w_{a3} and w_{a4} are the extracted watermarks and $i_{wa1LUpos}$, $i_{wa2LDpos}$, $i_{wa3RUpos}$, $i_{wa4RDpos}$ are the attacked watermarked image in the FCA concept positions. Figure 9 illustrates the extraction scheme for our approach.

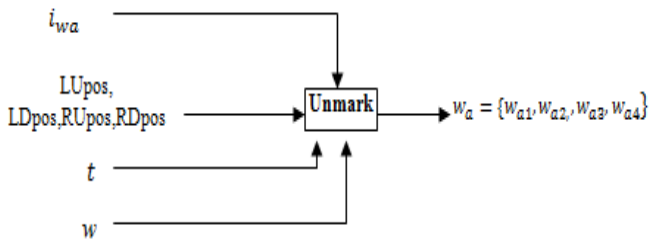


Figure 9. Watermark Extraction Scheme

The extraction steps can be summarized in the following algorithm (algorithm IV).

Algorithm IV

INPUT: i_{wa} (attacked watermarked image), (w_1, w_2, w_3, w_4) position(LU_FCA, LD_FCA, RU_FCA, RD_FCA)

OUTPUT: $w_{a1}, w_{a2}, w_{a3}, w_{a4}$ (attacked watermark images)

```

for each item in  $w_1$  watermark
     $w_{a1} = (1/t) * w_1 - (1-t/t) * i_{wa}(\text{position}(\text{LU\_FCA}))$ 
for each item in  $w_2$  watermark
     $w_{a2} = (1/t) * w_2 - (1-t/t) * i_{wa}(\text{position}(\text{LD\_FCA}))$ 
for each item in  $w_3$  watermark
     $w_{a3} = (1/t) * w_3 - (1-t/t) * i_{wa}(\text{position}(\text{RU\_FCA}))$ 
for each item in  $w_4$  watermark
     $w_{a4} = (1/t) * w_4 - (1-t/t) * i_{wa}(\text{position}(\text{RD\_FCA}))$ 

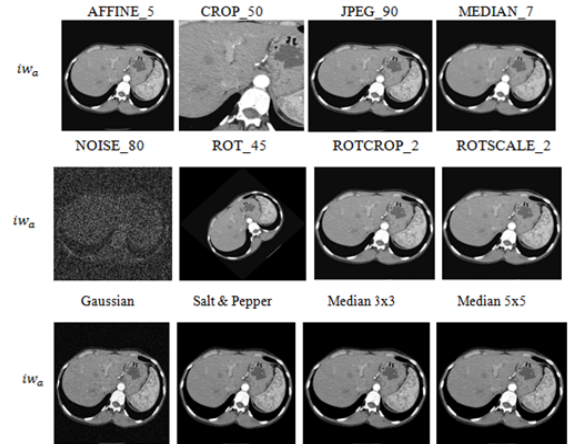
```

save $w_{a1}, w_{a2}, w_{a3}, w_{a4}$

end

IV. EXPERIMENTAL RESULTS

We performed our tests on a database of 100 DICOM images and here we took as an example the stomach CT medical database images of size 512×512 . The original images come from [21] while the watermark contains the four watermark images built from the header of the medical image. The watermarking process has as the secret key t , which varies exclusively between 0 and 1 in order to achieve visible and invisible watermarking. Similarly, we tested our proposed watermarking algorithm against several kinds of attacks, introduced using StirMark Benchmark [22, 23], such as median filtering, JPEG compression, rotation, etc... We added Gaussian, salt and pepper noise and other attacks as shown in figure 10 A, figure 10 B shows the retrieved attacked watermarks. Through the obtained results we concluded that the invisible watermarking (t close to 1) gives better results than the visible one ($t = 0.02$) as we can show in figure 8.



A



Figure 10. Attacked watermark and retrieved watermark images
A Attacked watermark image with $t = 0.98$
B Retrieved the attacked watermark images with $t = 0.98$

To evaluate the retrieved watermark image quality in relation to the original watermark image, we calculated the Mean Square Error (MSE)[24], Peak Signal-to-Noise Ratio (PSNR) [25] and the Normalized Cross Correlation (NCC) metrics [26]. The following formulas were used:

$$PSNR(w, w_a) = 10 \log_{10} \left(\frac{(2^P - 1)^2}{MSE} \right) \quad (16)$$

$$MSE(w, w_a) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (w(i, j) - w_a(i, j))^2 \quad (17)$$

$$MSE(w, w_a) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (w(i, j) - w_a(i, j))^2 \quad (18)$$

Where w and w_a , denote the original watermark and the extracted watermark image, respectively. P is the image depth, $M \times N$ is the image size. In our approach, the PSNR calculation was done between w_1, w_2, w_3, w_4 and $w_{a1}, w_{a2}, w_{a3}, w_{a4}$, respectively.

A. Robustness

Table 3 shows the PSNR values for the extracted watermark from the attacked watermarked image after geometric and non-geometric attacks made with Stirmark, compared with the original watermark. We compared our results with the proposed methods in [11, 27, 28]. Our proposed scheme outperforms the algorithms introduced in [11, 27, 28].

In order to further verify the robustness under image processing operations, we added Gaussian, salt and pepper noise, JPEG compression with quality factors 60 and 90, and image filtering as 3×3 and 5×5 , used in methods [2], [11] and [28]. Table 4 lists the results of adding noise, which means that our proposed algorithm has stronger robustness. The metric used to measure the quality is a Normalized Cross Correlation (NCC).

TABLE III. QUALITY MEASUREMENTS FOR EXTRACTED WATERMARK AFTER ATTACKS

PSNR	AFFINE_5	CROP_50	JPEG_90	MEDIAN_7
w_{a1}	48.4227	41.4469	45.6388	45.7755
w_{a2}	41.8699	43.8399	41.9063	43.6029
w_{a3}	39.4454	38.5097	41.4123	41.0731
w_{a4}	45.5536	39.0599	46.3968	47.1297
[11]	29.65	27.65	29.27	30.31
[27]	16.58	13.38	26.93	27.25
[28]	11.56	10.50	17.61	18.64
PSNR	NOISE_80	ROT_45	ROTCROP_2	ROTSKALE_2
w_{a1}	47.3029	52.2202	47.3536	43.7296
w_{a2}	43.3088	40.6519	42.5764	41.5464
w_{a3}	39.9710	36.9476	39.3824	37.8864
w_{a4}	42.0503	38.8461	42.1563	44.9723
[11]	12.12	11.58	13.56	14.53
[27]	33.14	31.56	33.55	33.72
[28]	7.93	18.65	19.21	19.18

TABLE IV. NCC RESULTS AFTER COMMON IMAGE PROCESSING ATTACKS

NCC		Gaussian	Salt & pepper	JPEG		Median Filter	
				60	90	3 x 3	5 x 5
Proposed approach	w1	0.9987	0.9980	0.9987	0.9988	0.9980	0.9980
	w2	0.9995	0.9989	0.9989	0.9988	0.9991	0.9991
	w3	0.9990	0.9988	0.9983	0.9983	.9988	0.9992
	w4	0.9993	.9994	0.9996	0.9996	0.9993	0.9993
[2]		0.9633	0.9413	0.9681	0.9980	0.9965	0.9273
[11]		0.88	0.92	0.96	0.99	0.90	0.76
[28]		0.93	0.93	0.93	0.93	0.91	0.92

From the above results in tables 3 and 4, we can conclude that our proposed method has a stronger robustness against geometric, non-geometric and common image processing attacks.

B. Capacity

Our watermark consists of four watermark images. After applying various attacks as we see in figure 10, we can retrieve the watermark. Even though there are degradations in the watermark image quality, we still have the possibility to retrieve the watermark. Our approach provides a low capacity. This is because the watermark that is embedded is very small in terms of size compared with the original image size and in comparison with the works in [2] [11] [28], as we can see in table 5. Our original image size is 512×512 .

TABLE V. THE BITS USED FOR THE WATERMARK IMAGE

		Watermark size	
Proposed Approach	W_1	200	Total = 880 bits
	W_2	312	
	W_3	152	
	W_4	216	
[2]		4096	
[11]		1056	
[28]		1024	

[1] C. I. PODILCHUK AND E. J. DELP, "DIGITAL WATERMARKING: ALGORITHM AND APPLICATION," IEEE SIGNAL PROCESSING MAGAZINE, VOL. 18, NO. 4, PP.33–46, (2001).

[2] Q. SU, Y. NIU, Q. WANG & G. SHENG "A BLIND COLOR IMAGE WATERMARKING BASED ON DC COMPONENT IN THE SPATIAL DOMAIN." OPTIK-INTERNATIONAL JOURNAL FOR LIGHT AND ELECTRON OPTICS 124.23 (2013): 6255-6260.

C. Complexity

In terms of measuring the complexity with the proposed approach, we calculated the execution time for the embedding and extraction process using MATLAB 7.14 with a CPU of 2.4 GHz and 2 GB RAM. Our proposed approach has a lower complexity than [2]. Table 6 shows the execution time for embedding and extraction processes for our proposed methods and those of [2].

TABLE VI. COMPARISONS OF THE EXECUTION TIME BETWEEN THE PROPOSED METHOD AND THE METHOD IN [2]

Time	Proposed method	[2]
Watermark embedding time	0.4125	0.5244
Watermark extraction time	0.3392	0.3701
Total time	0.7517	0.8945

D. Tamper Detection

Moreover, we can also detect if there have been removal attacks or the addition of any new watermarks. By subtracting the fourth watermark from the second watermark, our approach gives us the third watermark. By comparing the subtraction result with the third watermark, we can know if any removal or addition has taken place. For instance, after the extraction phase, we obtained four watermarks $w_{a1}, w_{a2}, w_{a3}, w_{a4}$. By subtracting the w_{a4} (File Modified Date) from w_{a2} . (Patient Date Of Birth), the result should be the patient age, this value is equal to w_{a3} .

V. CONCLUSION

We presented a reversible novel watermarking approach in the spatial domain. Our approach is innovative and based on using Formal Concept Analysis to generate the optimal position for embedding. The watermark is built from some header information of the DICOM image. It is embedded into the NROI of the medical image. Based on experimental results, our approach demonstrates a lower computational complexity, using low capacity for the watermark and has a high robustness. Moreover, the approach can detect the removal and/or addition and/or replacement during attacks, which would be useful for tamper detection issues. Although the proposed approach has been limited in this paper to medical image, it could be used with other kinds of images.

REFERENCES

- [3] L. Priya, and V. Sadasivm. "A Survey on watermarking techniques, requirements, applications for medical image". Journal of Theoretical and Applied Information Technology 65.1 (2014).
- [4] L. Kobayashi, O. Massato, S. Furuie, and P. Messeder. "Providing integrity and authenticity in DICOM images: A novel approach." Information Technology in Biomedicine, IEEE Transactions on 13.4 (2009): 582-589.
- [5] Subramanyam, S. Emmanuel & M. Kankanalli, "Robust watermarking of compressed and encrypted JPEG2000 images". Multimedia, IEEE Transactions on, 14(3), 703-716.(2012).
- [6] Cancellaro, M., Battisti, F., Carli, M., Boato, G., De Natale, F. G., & Neri, A. "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain". Signal Processing: Image Communication, 26(1), 1-12. (2011).
- [7] Mousavi, S. M., Naghsh, A., & Abu-Bakar, S. A. R. "Watermarking techniques used in medical images: a survey". Journal of digital imaging, 27(6), 714-729. (2014).
- [8] S.Wang, , D. Zheng,, J. Zhao,W. Tam, & F. Speranza, "Adaptive watermarking and tree structure based image quality estimation". Multimedia, IEEE Transactions on, 16(2), 311-325. (2014).
- [9] P. Korus, J. Bialas& A. Dziech, "Towards Practical Self-Embedding for JPEG-compressed Digital Images". Multimedia, IEEE Transactions on, (2015).
- [10] H. Lin, W. Wang, Y. R. Horng, S. J. Kao, & Y. Pan, "A blind watermarking method using maximum wavelet coefficient quantization." Expert Systems with Applications 36.9 (2009): 11509-11516.
- [11] J. Li, , C. Dong, M. Huang, H. Zhang, & W.. "A Novel Robust Watermarking for Medical Image."Advances in Information Sciences & Service Sciences 4.11 (2012).
- [12] M. Kutter, and S. Winkler, A vision-based masking model for spread-spectrum image watermarking, Journal of IEEE Trans. Image Processing, vol. 11, no. 1, pp. 16-25, (2002).
- [13] M. Peter, M. Eichelberg, and E. Martin. "Introduction to the DICOM standard." European radiology 12.4 (2002): 920-927.
- [14] N. Memon. and S. Gilani, "NROI watermarking of medical images for content authentication." Multitopic Conference, 2008. INMIC 2008. IEEE International. IEEE, 2008.
- [15] F. Alqadah, , and R. Bhatnagar. "Similarity measures in formal concept analysis." Annals of Mathematics and Artificial Intelligence 61.3 (2011): 245-256.
- [16] W. Rudolf. "Concept lattices and conceptual knowledge systems."Computers & mathematics with applications 23.6 (1992): 493-515.
- [17] D. Richards, and P. Compton, (1997). Combining formal concept analysis and ripple down rules to support reuse, software engineering knowledge engineering SEKE'97. Springer Verlag.
- [18] G. Jiang, K.Ogasawara, A. Endoh, & T. Sakurai, "Context-based ontology building support in clinical domains using formal concept analysis". International Journal of Medical Informatics Journal, 71, 71-81.(2003)
- [19] G. Bernhard, G. Stumme, and R. Wille, eds. Formal Concept Analysis: foundations and applications. Vol. 3626. springer, (2005).
- [20] Z. Emmanuel, and M. Samuelides. "Galois Lattice Theory for Probabilistic Visual Landmarks." J. UCS 10.8 (2004): 1014-1033.
- [21] <http://www.dicomlibrary.com/>
- [22] Fabien, P. Petitcolas, J. Ross ,G. Markus " Attacks on Copyright Marking Systems", in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH'98, Portland, Oregon, U.S.A., April 15-17, (1998), Proceedings, LNCS 1525 , Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239.
- [23] Fabien, P. Petitcolas, " Watermarking Schemes Evaluation" IEEE Signal Processing, vol. 17, no. 5, pp. 58-64, September (2000).
- [24] Z. Wang and C. Alan. "A universal image quality index." Signal Processing Letters, IEEE 9.3 (2002): 81-84.
- [25] H. Quan, and M. Ghanbari. "Scope of validity of PSNR in image/video quality assessment." Electronics letters 44.13 (2008): 800-801.
- [26] Avants, C. Epstein, M. Grossman, & C. Gee, "Symmetric diffeomorphic image registration with cross-correlation: evaluating automated labeling of elderly and neurodegenerative brain." Medical image analysis 12.1 (2008): 26-41.

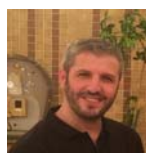
- [27] T. Hung-Hsu, Y. Jhuang, and Y. Lai. "An SVD-based image watermarking in wavelet domain using SVR and PSO." Applied Soft Computing 12.8 (2012): 2442-2453.
- [28] S. Miao, J. Li, Y. Bai, & W. Chen "Robust watermarking for medical images based on Arnold scrambling and DWT-DFT." Computing and Convergence Technology (ICCT), 2012 7th International Conference on. IEEE, 2012.

AUTHORS PROFILE



Muath AlShaikh is an Ph.D. student in Computer Science since 2013, University of Bretagne Occidentale, France. He received his Master degree in computer science in 2010 from Utara University in Malaysia and his B.Sc in computer science in 2006 from AlBalqa University, Jordan. He is affiliated to Lab-STICC / UMR CNRS 6283,

SFIIS team of the University of Bretagne Occidentale, France. His research interests include image and video watermarking, cryptology, information security, image processing and computer vision.



Lamri Laouamer is an assistant professor at the department of Management Information Systems, College of Business and Economics at Qassim University, KSA. He is also an associate researcher in Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance (Lab-STICC), University of Bretagne Occidentale, Brest, France. He received his Ph.D. in 2012 in computer science, field of Information security from the University of Bretagne Occidentale, France. His M.Sc. in 2006 in computer science and applied mathematics from the University of Quebec at Trois Rivieres in Canada. His B.Sc. in 1999 in computer science from the University of Setif, Algeria. His research interests include multimedia watermarking, cryptology and information security. Dr. Lamri Laouamer is an associate editor of the journal of Telecommunication systems by Springer and Associate editor of the Journal of Innovation in Digital Ecosystems by Elsevier.



Laurent NANA is Professor in Computer Science at the Computer Science Department of the Faculty of Science of University of Brest in France. He is member of the Team « Security, Reliability, Integrity of Information and Systems » of the Laboratory of Sciences and Techniques of Information, Communication and Knowledge (Lab-STICC / UMR CNRS 6283). His research interests include security of electronic data exchange, software for crisis management, languages and software architectures for safe control of remote systems.



PASCU Anca Christine is professor at the University of Bretagne Occidentale in Brest, France. She received her PhD in Mathematics from the University of Bucarest, Romania in 1977 and PhD in Computer Science Applied to Humanities from the University of Paris-Sorbonne in 2001. She passed her HDR (Habilitation à Dirigée des Recherches) in Paris-Sorbonne with the Logic of

Determination of Objects, a new non-classical logic applied to the language in 2006. Her research field is the logical models for the semantics of language and watermarking and cryptography as well.

Providing Quality of Service in Cognitive Radio Sensor Networks: A Survey

Sima Bemaninejad
Department of Computer Engineering
Yazd Azad University
Yazd, Iran

Abstract—Cognitive radio (CR) technology is an excellent solution to use dynamic spectrum access (DSA) technique with the aim of resolving the spectrum underutilization problems and spectrum scarcity problems in networks. Nowadays, wireless sensor networks (WSNs) are utilized in enormous applications. The unlicensed ISM spectrum bands are used for data communication in WSNs in most applications. Due to event-triggered traffic type of WSNs, these networks commonly meet the spectrum shortage in transmission of event information. This problem is solved by providing the CR-equipped sensors for WSNs. These networks are named as cognitive radio sensor networks (CRSNs). On account of WSNs' applications, these networks usually have some properties like limited battery power of sensors, real-time and repetitive traffic, etc. Owing to dynamic spectrum availability in CRSNs, supporting the quality of service (QoS) on CRSNs is a great challenge. Consequently, providing the QoS in CRSNs is an essential result and considerable issue. This paper presents a survey of recent studies in providing the QoS of CRSNs. The schemes who provide QoS are classified based on three types of classifications: First, based on QoS metrics, second, based on the approach types which are cross-layer and single-layer, third, based on type of schemes which are distributed, centralized and cluster-based, in this paper.

I. INTRODUCTION

Cognitive radio (CR) technology has the advantage of using the wireless spectrum bands opportunistically, which is a tremendous solution for the spectrum scarcity in wireless networks [1]. A wireless network with the CR technology equipped nodes is named cognitive radio networks (CRNs). These nodes are named as secondary users (SUs). Taking the advantages of CR technology, SUs use the unlicensed channels for data transmission. The licensed users of these CR channels are named as primary users (PUs) [2]. The SUs can use the CR channels in the absence of PUs thus the PUs have the priority to SUs. Each SU operates according to the cognitive radio operation cycle, which includes four operations: spectrum sensing, spectrum decision, spectrum hand-off, spectrum sharing [3]. On the other hand, each SU operates in two operating modes periodically: sensing mode and operating mode.

These days, the wireless sensor networks (WSNs) are the undeniable part of daily life due to the wide range of

applications in monitoring, object tracking, healthcare, home and industrial automation, security, emergency response etc. [4]. The features and applications of WSNs provide an appropriate platform to be considered as one of the main parts of the internet of things (IoT) which all the devices are connected to the internet to be controlled anywhere [5].

There are a lot of challenges in the operations of WSNs in different applications such as energy scarcity, spectrum scarcity, self-organizing features in the monitoring of harsh environments and inaccessible areas in these environments etc. The CR technology can be a fruitful solution to the spectrum scarcity of WSNs. The WSNs with CR equipped sensor nodes are named cognitive radio sensor networks (CRSNs) [6] and these CR equipped sensor nodes are named CR sensors. The CRSNs can benefit from some advantages of the dynamic spectrum access feature of CR technology. These advantages can be mentioned as the opportunistic use of spectrum bands for burst traffic, adapting sensors' operational modes to PU activity parameters in order to reduce power consumption and reduction of the development cost of the network by using the dynamic spectrum bands etc. [6].

There are two survey papers in CRSNs. In [6], the authors introduced the main principals, network design architectures and application areas of CRSNs. Also, all aspects, features and the open research issues and avenues in different layers of these networks are explained. The authors of [7] summarized all the recent studies about resource allocation in CRSNs. The advantages of these studies are described and the proposed schemes of these studies are classified into three categories, i.e, centralized, cluster-based and distributed in [7].

Since SUs can use the CR channels in the absence of PUs, SUs' data transmission depends on the PU activity parameters. Thus, the channel availability is highly variable for SUs. Due to this highly dynamic resource availability in CRSNs, providing the quality of service (QoS) of CRSNs' users in various applications is an excessive challenge. There are several studies in this area in order to guarantee the QoS measures of considered applications.

In this paper, the recent studies in the area of providing QoS of CRSNs' applications are summarized and categorized based on two different classification criteria. The first classification is based on QoS metric, i.e, delay, distortion, packet loss,

reliability, etc. The second classification is based on approach of design which is cross-layer approach or single-layer approach. The third classification is based on the type of proposed schemes which is distributed, centralized and cluster-based.

In the rest of the paper, the Section II gives an overview of CRSNs. The Section III summarizes the recent studies in the area of providing QoS. Finally, the Section IV concludes the paper. Ease of Use

II. OVERVIEW OF COGNITIVE RADIO SENSOR NETWORKS

In this section, the overall features of CRSNs' operation which relates to CR technology and sensors 'operations are described.

In CRNs, there are two approaches by SUs to access the spectrum: spectrum overlay and spectrum underlay [1]. The spectrum underlay approach allows the data transmission of both the PUs and SUs at the same time. In the spectrum overlay approach, the data transmission of SUs in the absence of PUs is allowed. In this paper the overlay approach is noticeable. However, to the best of our knowledge, there is no study based on underlay approach which provides QoS of CRSNs' applications.

There are two types of sensing operation in CRSNs: event sensing and spectrum sensing. Event sensing is carried out to detect event occurrence in the event area. Spectrum sensing is carried out to detect the presence of PUs periodically. The detail of the cognitive radio operation cycle is described in section II-A.

A. Cognitive Radio Operation Cycle

Spectrum Sensing: A SU needs to sense the wireless spectrum for predefined sensing time duration and check the presence of related PUs who has the license to use the considered spectrum channels. Since an SU cannot sense the CR channel and send data to it simultaneously, the spectrum sensing is done periodically with a predefined period with the aim of minimizing the amount of interference between the communication of SUs and PUs [3].

Spectrum Decision: This operation relates to the selection Of best free channel from the list of detecting free channels according to a considered criterion.

Spectrum hand-off: After selection of the appropriate spectrum band, the SU starts communication. However, due to the dynamic nature of CR channels, after a while, a PU may start communication in the selected channel. In this case, the SU changes its operating channel to avoid interference to the PU.

Spectrum Sharing: Several SUs can have access to the detected free CR channels. However, the access of two or more SUs to the same CR channel leads to collisions, and contention. Spectrum sharing manages the CR channel usage among multiple SUs to minimize the harmful collisions and interference.

The SUs are in two operational modes periodically. These modes are sensing mode and operational mode. The duration of these operational modes is specified. Data transmission is

performed in the operational mode in addition to considering the status of considered CR channels (spectrum hand-off, spectrum sharing and spectrum decision). The ideal sensing is assumed without any errors in the detection PU presence.

B. Primary User Activity

PUs have higher priority to use the CR channels. Modeling of PU activity has a high degree of importance [8] because of its impact on the communications of CR users. The most common model for PU activity is the two-state birth/death Markov process [8]. In CRNs, two states of Markov process are named ON and OFF states [1]. The wireless channel is busy by the PU (the PU is active on the CR channel) in the ON state. The PU is not active on the CR channel in the OFF state. The birth rate and death rate of these two state of Markov are called the entrance and departure rates of PUs, respectively.

The number of CR channels is highly effective in the performance of CRNs. For each CR channel, there is a licensed PU which enters this CR channel with a predefined mean entrance rate and leaves it with a predefined mean departure rate.

III. CLASSIFICATION OF RECENT RELATED STUDIES

In this study, all the proposed schemes to provide the QoS of the CRSNs' applications are reviewed and investigated. First, these schemes are categorized into several QoS metric criteria. Then, these schemes are categorized into two categories, cross-layer approach and single-layer approaches. Furthermore, these studies are classified under three category scheme types, distributed, centralized and cluster-based.

A. Considered QoS metrics

In [9], a cross-layer approach is proposed to provide the QoS desires in smart grid applications of CRSNs. The aim of this proposed approach is modeled as an optimization problem and a heuristic scheme is proposed as a cross-layer solution among physical, MAC and network layers. The priority of data flows is determined based on data rate, latency and reliability QoS requirements. According to the priority of data flows and based on the capacity and interference of channels, the appropriate channel is selected and also the routing protocol works based on interactions with MAC and physical layers.

The authors of [9] extended their research and designed a framework in [10] in order to control the power and provide QoS in CRSNs with smart grid applications. Dynamic spectrum access is performed in order to find the best channel in channel impairment conditions. A traffic management is performed which gives the flows' priorities based on data rate, data reliability (bit error rate (BER)) and latency factors. In order to maximize the network utility, this framework is formulated as an optimization problem. A suboptimal heuristic algorithm is proposed in order to support the QoS requirements of various smart grid applications by means of some decisions in flow control, channel control, routing and scheduling.

A traffic management mechanism is proposed in [11] for a cluster based CRSN in order to guarantee the delay constraint of real-time traffic. A reservation policy is introduced to support the QoS requirement of traffic types which are real-time and best effort traffic types. A part of bandwidth is reserved for real-time traffic by this policy. The delay of these traffic types and also transmission latency of inter and intra cluster traffics are analyzed in this study and this analysis is verified by NS2-based simulations [12]. This traffic management improves the spectrum utilization.

There are some proposed routing schemes in different kinds of cognitive radio networks like [33]. In [13], the authors proposed an energy efficient multimedia routing protocol according to spectrum information. A node clustering algorithm is introduced with the aim of limiting the nodes in node establishment base on history of usage of channels and the information of channel sensing. The node with higher residual energy and higher channel score is selected as cluster head. In order to minimize the packet loss and delay and then optimize the distortion of multimedia packets, the optimal number of clusters is determined in this routing protocol. In this routing, the TDMA and CSMA are used for intra-cluster and inter-cluster routing, respectively.

The aim of paper [14] is to optimize the spectrum efficiency and end to end delay in CRSNs. The spectrum efficiency is the gained throughput per bandwidth usage. The distributed source coding method (in-network processing) is used to reduce the CRSNs' traffic amount by reducing the repetitive sensor data. In addition, the upper and lower bounds of network capacity are calculated by graph theory approach. The packet delay of this network is analyzed, then, according to the considered QoS requirements, the throughput and throughput gain with a guarantee of delay requirement is derived.

Since, the QoS requirements like minimizing power consumption in transmissions, maximizing throughput and minimizing the interference of SUs' transmissions on PUs' transmission has confliction to each other, the authors of [15] proposed a multi-objective evolutionary algorithm in order to provide these QoS requirements. The proposed algorithm is named as Non-dominated Sorting Genetic Algorithm (NSGA-II) which obtained superiority to ordinary genetic algorithm in packet delivery ratio, average throughput, spectrum opportunity utilization, end to-end delay, average interference ratio, and network lifetime.

In [16], the channel allocation approach is proposed in CRSNs with considering the QoS requirements of complete coverage and minimum power consumption, data rate and interference. This approach is modeled by a Mixed Integer Non-Linear Programming (MINLP) optimization problem. This problem is relaxed to a linear programming (LP) problem. Three heuristic algorithms are proposed for channel assignment in order to reduce the computational complexity.

The authors of [17] proposed a video streaming mechanism for CRSNs which is named as "EMCOS: Energy-

efficient Mechanism for Multimedia Streaming over Cognitive Radio Sensor Networks". This mechanism provides high quality transmission of real time multimedia data considering the power consumption aspects of CRSNs' nodes. In order to reduce the energy consumption of transmissions, a clustering approach is proposed. Also, in order to provide the content delivery to the sink node, a routing mechanism in addition to the channel selection mechanism is proposed. These mechanisms lead to providing lower end-to-end delay, lower frame loss ratio under unstable CR channel conditions and higher video quality.

In [18], an interference model is proposed in underlay CRSNs which SUS and PUs communicate simultaneously. According to this interference model, a power control is presented in order to keep the interference and SINR value of these nodes under a predefined constant in these networks. The aim of this power control is to maximize throughput and energy efficiency.

The authors of [19] extended their research and presented a performance analysis of real-time traffic in CRSNs in [20]. Two types of real-time traffic and also two kinds of spectrum handoff are considered in this study. The average transmission delay is calculated for these considered real-time traffics and spectrum handoff types.

The authors of [21] present an analytical model for the steady state sending rate of sensor nodes based on the operation of AIMD and AIAD congestion control methods in CRSNs. The sending rate of sensor nodes is modeled by discrete time Markov chain (DTMC). According to this sending rate model and general probability density functions (PDFs) of input rate, the queue length of sensor nodes is modeled by semi-Markov chain (SMC). These models are verified by NS2-cognitive radio based simulation framework [22].

In [23], in order to enhance the network lifetime and spectrum utilization in CRSNs, two adaptation techniques are proposed. The first technique is adapting the packet size to CR channel states and the second technique is the assignment of channels based on the residual power of the sensors.

The authors of [24] proposed a central sleep scheduling mechanism in order to enhance the network lifetime in CRSNs. In this scheduling mechanism, the duty cycle of nodes composes of sensing time, sleep time and transmission time. This scheduling mechanism leads to improve the spectrum efficiency and the network lifetime.

In [25], the significant principals and challenges of CRSNs are explored in smart grid applications with real-time traffic. Different proposed transport algorithms of WSNs and CRNs are investigated. These evaluations support ideas about real-time transport protocols in CRSNs in smart grid applications.

In [26], the stochastic backlog and delay bounds of AIMD congestion control scheme are analyzed based on stochastic network calculus. In this analysis the moment generating functions are used to model these delay and backlog bounds.

The author of [27] formulated bandwidth and delay as two important QoS metrics in CRSNs. These metrics are evaluated in a CSMA MAC protocol using a common control channel based on the point that SUs can use CR channels concurrently in the joint interference region. Using the common control channel leads to enhance delay and aggregated bandwidth.

In [28], the authors investigated the reliability and affecting factors in cognitive radio sensor actor networks. They presented a cooperative sensing method in order to achieve the global information about CR channels. The simulation results show this cooperation improves the reliability of PUs' transmission in these networks.

Table 1: The summary of all QoS provision schemes

survey	QoS metric	Scheme type	Approach
[9],[10]	Delay, Bandwidth, BER	Distributed	Cross-layer
[11]	Delay	Cluster-based	Single-layer
[13]	Distortion, Packet losses, Latency	Cluster-based	Cross-layer
[14]	Delay	Distributed	Cross-layer
[15]	Power, Throughput, Interference	Centralized	Cross-layer
[16]	Power, Interference	Centralized	Single-layer
[17]	End-to-end delay, Frame loss ratio	Cluster-based	Cross-layer
[18]	Interference, SINR	Centralized	Single-layer
[19], [20]	Delay	Centralized	Single-layer
[21]	Delay	Distributed	Cross-layer
[23]	Power, Spectrum utilization	Distributed	Single-layer
[24]	Spectrum efficiency, Lifetime	Distributed	Single-layer
[26]	Backlog and delay	Centralized	Cross-layer
[27]	Bandwidth, Delay	Centralized	Single-layer
[28]	Interference, (reliability of PUs')	Centralized	Single-layer
[30]	Delay	Cluster-based	Single-layer
[31]	Lifetime, Throughput	Cluster-based	Cross-layer
[32]	Delay, Jitter	Centralized	Cross-layer
[34]	Delay	Distributed	Cross-layer

In [29], the performance of existing transport protocols is analyzed. This analysis demonstrates the CRSN specific transport protocols are essential. Some open problem and challenges for the transport layer of CRSNs are introduced in this paper.

In [30], a MAC protocol is proposed in order to provide some QoS metrics in cluster based CRSNs. A backup channel is considered for sudden spectrum back-off. The priorities of the cluster members are determined based on the delay constraint of data packets.

The authors of [31] proposed a spectrum-aware version of the LEACH protocol, which is named as cognitive radio Low Energy Adaptive Clustering Hierarchy (CogLEACH). This protocol selects the cluster heads based on the number of free CR channels of the nodes. This proposed protocol leads to higher lifetime and the throughput of the network.

In [32], a connection admission control is presented in CRSNs with multimedia applications in order to enhance delay and jitter of data packets. This mechanism is modeled as a binary integer programming problem and is solved by a branch and bound heuristic method.

The performance of the mentioned proposed congestion model in [21] is evaluated in [34]. In [34], a metric as rate-congestion ratio (RCR) is defined. The aim is to achieve the maximized value of RCR in the networks with AIMD and AIAD congestion control methods.

A summary of these surveyed papers is presented in table1. Three considered classifications of these studies are determined in this table.

IV. CONCLUSION

In this paper, the recent studies who propose schemes to support QoS for CRSNs have been surveyed. These schemes are categorized under three types of categories and a review of these categories is presented. The first category divides studies based on considered QoS metrics which are delay, bandwidth, BER, interference, power, packet loss, jitter or a combination of these metrics. The second category divides recent studies of this field into two types: cross-layer and single-layer approaches. The third category divides recent proposed schemes into distributed, centralized and cluster-based scheme types.

REFERENCES

- [1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, Sep. 2006.
- [2] J. Mitola, J. Maguire, G.Q., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, col. 6, no. 4, pp. 13-18, 1999.
- [3] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury, "Spectrum management in cognitive radio ad hoc networks," *IEEE Network*, vol. 23, no. 4, pp. 6-12, Jul. 2009.
- [4] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," *International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2001)*, Salt Lake City, Utah, pp. 2033-2036, May 2001.
- [5] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A survey", *Computer Networks*, Volume 54, Issue 15, 28 October 2010, Pages 2787-2805.
- [6] O. Akan, O. Karli, O. Ergul, *Cognitive radio sensor networks*, *IEEE Network* 23, no. 4, pp. 34-40. 2009.

- [7] A. Ahmad, S. Ahmad, M. H. Rehmani, and N. U. Hassan, "A Survey on Radio Resource Allocation in Cognitive Radio Sensor Networks," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 888–917, Secondquarter 2015.
- [8] W.-Y. Lee, I. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, 2008.
- [9] G. A. Shah, V. C. Gungor, and O. B. Akan, "A cross-layer design for QoS support in cognitive radio sensor networks for smart grid applications," in *2012 IEEE International Conference on Communications (ICC)*, 2012, pp. 1378–1382.
- [10] G. A. Shah, V. C. Gungor, and O. B. Akan, "A Cross-Layer QoS-Aware Communication Framework in Cognitive Radio Sensor Networks for Smart Grid Applications," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1477–1485, Aug. 2013.
- [11] L. Li, N. Li, W. Xie, and Y. Xu, "Delay performance evaluation for supporting heterogeneous traffic in cognitive radio sensor networks," in *2013 International Conference on Information Science and Technology (ICIST)*, 2013, pp. 1455–1459.
- [12] Network simulator version 2. (<http://www.isi.edu/nsnam/ns/>).
- [13] G. A. Shah, F. Alagoz, E. A. Fadel, and O. B. Akan, "A Spectrum-Aware Clustering for Efficient Multimedia Routing in Cognitive Radio Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3369–3380, Sep. 2014.
- [14] S.-C. Lin and K.-C. Chen, "Improving Spectrum Efficiency via In-Network Computations in Cognitive Radio Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1222–1234, Mar. 2014.
- [15] T. M. Salem, S. Abdel-Mageid, S. M. Abd El-kader, and M. Zaki, "A quality of service distributed optimizer for Cognitive Radio Sensor Networks," *Pervasive and Mobile Computing*, vol. 22, pp. 71–89, Sep. 2015.
- [16] R. M. Eletreby, H. M. Elsayed, and M. M. Khairy, "Optimal spectrum assignment for cognitive radio sensor networks under coverage constraint," *IET Communications*, vol. 8, no. 18, pp. 3318–3325, 2014.
- [17] A. Bradai, K. Singh, A. Rachedi, and T. Ahmed, "EMCOS: Energy-efficient Mechanism for Multimedia Streaming over Cognitive Radio Sensor Networks," *Pervasive and Mobile Computing*, vol. 22, pp. 16–32, Sep. 2015.
- [18] T. M. Phuong and D.-S. Kim, "Efficient power control scheme for cognitive industrial sensor networks," *International Journal of Control and Automation*, vol. 7, no. 3, pp. 177–188, 2014.
- [19] Z. Liang and D. Zhao, "Quality of Service Performance of a Cognitive Radio Sensor Network," in *2010 IEEE International Conference on Communications (ICC)*, 2010, pp. 1–5.
- [20] Z. Liang, S. Feng, D. Zhao, and X. Shen, "Delay Performance Analysis for Supporting Real-Time Traffic in a Cognitive Radio Sensor Network," *IEEE Transactions on Wireless Communications*, vol. 10, no. 1, pp. 325–335, Jan. 2011.
- [21] V. Esmaealzadeh, E. S. Hosseini, R. Berangi, and O. B. Akan, "Modeling of Rate-based Congestion Control Schemes in Cognitive Radio Sensor Networks," *Ad Hoc Networks*, vol. 36, Part 1, pp. 177–188, Jan. 2016.
- [22] V. Esmaealzadeh, R. Berangi, S. M. Sebt, E. S. Hosseini, and M. Parsinia, "CogNS: A Simulation Framework for Cognitive Radio Networks," *Wireless Personal Communications*, vol. 72, no. 4, pp. 2849–2865, Apr. 2013.
- [23] X. Li, D. Wang, J. McNair, and J. Chen, "Dynamic spectrum access with packet size adaptation and residual energy balancing for energy-constrained cognitive radio sensor networks," *Journal of Network and Computer Applications*, vol. 41, pp. 157–166, May 2014.
- [24] J. QIAO, J. LIU, W. WANG, and Y. ZHANG, "Spectrum-driven sleep scheduling algorithm based on reliable theory in cognitive radio sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, Supplement 2, pp. 47–72, Oct. 2012.
- [25] A. O. Bicen, V. C. Gungor, and O. B. Akan, "Delay-sensitive and multimedia communication in cognitive radio sensor networks," *Ad Hoc Networks*, vol. 10, no. 5, pp. 816–830, Jul. 2012.
- [26] V. Esmaealzadeh, R. Berangi, E. S. Hosseini, and O. B. Akan, "Stochastic Backlog and Delay Bounds of Generic Rate-based AIMD Congestion Control Scheme in Cognitive Radio Sensor Networks," *Pervasive and Mobile Computing*, vol. 22, no. C, pp. 46–57, Sep. 2015.
- [27] G. A. Shah and O. B. Akan, "Performance analysis of CSMA-based opportunistic medium access protocol in cognitive radio sensor networks," *Ad Hoc Networks*, vol. 15, pp. 4–13, Apr. 2014.
- [28] O. Ergul, A. O. Bicen, and O. B. Akan, "Opportunistic reliability for cognitive radio sensor actor networks in smart grid," *Ad Hoc Networks*.
- [29] A. O. Bicen and O. B. Akan, "Reliability and congestion control in cognitive radio sensor networks," *Ad Hoc Networks*, vol. 9, no. 7, pp. 1154–1164, Sep. 2011.
- [30] M. M. A. Pritom, S. Sarker, M. A. Razzaque, M. M. Hassan, M. A. Hossain, A. Alelaiwi, M. M. A. Pritom, S. Sarker, M. A. Razzaque, M. M. Hassan, M. A. Hossain, and A. Alelaiwi, "A Multiconstrained QoS Aware MAC Protocol for Cluster-Based Cognitive Radio Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2015, p. e262871, Apr. 2015.
- [31] R. M. Eletreby, H. M. Elsayed, and M. M. Khairy, "CogLEACH: A spectrum aware clustering protocol for cognitive radio sensor networks," in *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, 2014, pp. 179–184.
- [32] E. S. Hosseini, V. Esmaealzadeh, R. Berangi, and O. B. Akan, "A correlation-based and spectrum-aware admission control mechanism for multimedia streaming in cognitive radio sensor networks," *International Journal of Communication Systems*, in press, May 2015.
- [33] Abedi, O. and S. Bemaninejad. Soft and stable routing protocol for cognitive radio VANETs considering cognitive users mobility. in *Innovations in Information Technology (IIT)*, 2015 11th International Conference on. 2015.
- [34] V. Esmaealzadeh and R. Berangi, "On the Optimality of Generic Rate-based AIMD and AIAD Congestion Control Schemes in Cognitive Radio Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 614643, 2015.

iCloud and Its Security Issues in Relation with Find My iPhone

Sanjay Agal, *Associate Professor*, Sampreshita Maheshwari, *MTech Scholar*, *Pacific University*

Abstract— The iCloud technology is one of the recent and the most brilliant service created and hosted by the Apple Inc. Its main function is to serve as a backup system on all Apple products. The Find My iPhone application is the application, was formerly a part of the MobileMe architecture, which allows the users of the iPhone or other iDevices to track the location of their iPhone or other iDevices when it gets either lost or stolen. The user of the application will be able to see the iPhone's (almost) approximate location on the map, display a message onto the iPhone, and/or play a sound on the iPhone (even if the iPhone is on the silent mode), change the password on the iPhone, and also remotely erase the contents of the iPhone. The Find My iPhone application was made free of charge with iOS 4.2.1 software update, but this was only for devices introduced in 2010 and thereafter. There was another iOS app released by Apple around June 2010, which allowed the users to locate their device from another iOS devices running on iOS 4 or later. With every upgrade to the application or the software there was a new feature added which made the application more efficient in tracking the lost or stolen device. There are similar phone finder services or applications under various names, which are equally good enough, also are available for other types of smartphones.

Index Terms— Find my phone , apple m artificial intelligence

I. INTRODUCTION

Apple's Find My iPhone application is by-far the best available application in the market today to search and

locate the misplaced iPhone or other iDevices. However, no matter how good it is, it will still have bugs as it is nothing but a software program. When a mobile iDevice or the iPhone is stolen, the first thing that the robber would do is switch off the iPhone and then remove and crush the SIM card (present in the iPhone), so that it's not easy to locate it. Once the SIM card is out and the iPhone is switched off, it is practically impossible to locate it.

Another scenario is where the robber tries to switch on the device, without erasing it, the device asks for a password and will send an alert to Apple's support team. The owner of the device can also send an alert on the iPhone for searching it. The alerts will reach the device only if the device has some service provider data network or is connected to the Wi-Fi. Either of the condition should match to avail the service of finding the iPhone's Find My iPhone application. The third scenario is where no activation code is available or set by the owner and even the Find My iPhone application is not activated. In such cases nothing can be done as there is no remote access available to the iPhone for the owner. All of the above mentioned scenarios will be broadly presented in the following chapters of this dissertation along with the suggestions to overcome or partially resolve the problems caused in the smooth running of the application and the devices upon which the application is running. Apple's Find My iPhone application is by-far the best available application in the market today to search and locate the misplaced iPhone or other iDevices. However, no matter how good it is, it will still have bugs as it is nothing but a software program. When a

T. C. Author is with the Computer Science Department of Pacific University (e-mail: sanjayagal@pacific-university.ac.in).

mobile iDevice or the iPhone is stolen, the first thing that the robber would do is switch off the iPhone and then remove and crush the SIM card (present in the iPhone), so that it's not easy to locate it. Once the SIM card is out and the iPhone is switched off, it is practically impossible to locate it.

Another scenario is where the robber tries to switch on the device, without erasing it, the device asks for a password and will send an alert to Apple's support team. The owner of the device can also send an alert on the iPhone for searching it. The alerts will reach the device only if the device has some service provider data network or is connected to the Wi-Fi. Either of the condition should match to avail the service of finding the iPhone's Find My iPhone application. The third scenario is where no activation code is available or set by the owner and even the Find My iPhone application is not activated. In such cases nothing can be done as there is no remote access available to the iPhone for the owner. All of the above mentioned scenarios will be broadly presented in the following chapters of this dissertation along with the suggestions to overcome or partially resolve the problems caused in the smooth running of the application and the devices upon which the application is running.

Apple's Find My iPhone application is by-far the best available application in the market today to search and locate the misplaced iPhone or other iDevices. However, no matter how good it is, it will still have bugs as it is nothing but a software program. When a mobile iDevice or the iPhone is stolen, the first thing that the robber would do is switch off the iPhone and then remove and crush the SIM card (present in the iPhone), so that it's not easy to locate it. Once the SIM card is out and the iPhone is switched off, it is practically impossible to locate it.

Another scenario is where the robber tries to switch on the device, without erasing it, the device asks for a password and will send an alert to Apple's support team. The owner of the device can also send an alert on the iPhone for searching it. The alerts will reach the device only if the device has some service provider data network or is connected to the Wi-Fi.

Either of the condition should match to avail the service of finding the iPhone's Find My iPhone application. The third scenario is where no activation code is available or set by the owner and even the Find My iPhone application is not activated. In such cases nothing can be done as there is no remote access available to the iPhone for the owner. All of the above mentioned scenarios will be broadly presented in the following chapters of this dissertation along with the suggestions to overcome or partially resolve the problems caused in the smooth running of the application and the devices upon which the application is running.

II. OBJECTIVES

The main objective of the paper is to highlight and elaborate the following questions as well as to give a spotlight to those bugs and loopholes in the application which were found during the research, and suggest ways through various analysis to overcome the problems caused due to these loopholes:

- i. The first question for the research would be 'why to use this application?'
- ii. Then will come, how exactly is the device located using this application?
- iii. What are the benefits of this application?
- iv. How safe will the data be once the device is lost?
- v. If the application fails to locate the device, what can be done next?
- vi. What are the limitations of this application and how can we overcome these limitations?
- vii. Will the suggestions to overcome the limitations work in the real world as they would work in the ideal world?

The ultimate goal for this paper is try to make the device secure and locating the device more efficiently and

successfully. Also, suggesting ways to make the existing application function in a more robust manner.

III Analysis

We will start with the most basic question asked about the topic of this paper, which is, why is this application needed in the first place? The answer lies in the topic itself. The iPhone or any iDevice as a matter of fact is a very precious and expensive device and has tremendous value to the user. If the user loses the iPhone, they will strive hard to recover it back. To make things easier for the user, Apple Inc. has launched this Find my iPhone application. This makes the user's attempts to locate the device much more meaningful and may even lead to success depending on various factors.

Well, since the user knows that this application helps the user to track the iPhone; doesn't the user want to know how does it achieve this? When the iPhone is misplaced, the user has to log-in to the iCloud's web-based portal and has to use the online application of the Find my iPhone application. The last location of the user's phone is synced with the Apple's servers. If the phone is still active (that is alive and online) and is connected to the internet then one can perform various operations on it, such as Erase the iPhone, Lock the device, Play a sound, and Display a message and activate lost mode. The application uses the Wi-Fi connection or the mobile data connection to achieve this. It uses the phone's GPS service to accurately determine the phone's location. The analysis based on how did the web-based portal behave with the desired actions performed is mentioned below.

The first function is where the input is the button of Play Sound on the web portal after logging in the iCloud web portal. The output is displayed on the iPhone as well as an email is sent to the Apple ID email account of the user of the iPhone. The iPhone makes a loud noise so that the device can be located if it is near by the user. When the user selects play a sound option from the web portal, the user can hear a beeping tone on the phone with a message "Find My iPhone Alert" with an OK button available. If the user clicks on the OK

button the sound stops playing and the user can see the home screen of the iPhone.

The next function is where the input is the button of Lost Mode on the web portal after logging in the iCloud web portal. The output is displayed in the form of a lock on the iPhone as well as an email is sent to the Apple ID email account of the user of the iPhone. The iPhone is locked and no one but the user can use it. The iPhone can be unlocked only when the passcode is entered on the iPhone. And when the device is found, that is the iPhone which had gone offline has come online, a notification is sent to the email address of the user stating the location of the iPhone and when was it located. The iPhone can be tracked, once online, using the Find My iPhone web application and the device is tracked live while on the move. After the user has selected the Lost Mode option on the iCloud web portal, the phone gets locked and the person or the individual who has the device cannot perform any action on the phone. Optionally, we can also display a message with this feature.

The next function is where the input is the button of Erase iPhone on the web portal after logging in the iCloud web portal. The output for this scenario cannot be displayed as the iPhone was not erased. The iPhone is the in-use device of the owner and hence cannot be erased. After erasing the device, the user can delete the device from the list of devices on the user's iCloud account. When the iPhone is selected to be erased, the iPhone will restart and delete every file on the phone and will be as good as a factory reset. The user will no longer be able to track the iPhone, as this will erase the iCloud account from it.

The last function is where the input is the button of Lost Mode on the web portal after logging in the iCloud web portal. The output is displayed in the form of a lock on the iPhone as well as an email is sent to the Apple ID email account of the user of the iPhone. The iPhone is locked and no one but the user can use it. The iPhone can be unlocked only when the passcode is entered on the iPhone. A message is displayed on the screen of the iPhone. This a custom message and can be

edited by the user to get the iPhone back if anyone, who is sincere enough to give back the iPhone, finds it. When the lost mode option is selected, the iPhone displays a message on the lock screen itself, and if the user adds a phone number inside the message, any person who is in possession of the iPhone can call the user from the lock screen of the iPhone without the need of unlocking the iPhone.

IV Results

The statistical analysis is the output for the paper where the research is computed into statistical functions and a calculated output is generated based on the statistical data generated. Statistics, as per the definition, is the study of the collection, analysis, interpretation, presentation, and organization of the data obtained during the research. The statistical analysis for the paper is based upon the probability of the success rate that is generated as the result of the research. The data is computed based upon the fact whether the iPhone is available as offline or online.

The result of this statistical analysis and testing is dependent on the answers of the research questions and scenarios that were computed into statistical functions and a calculated output was generated based on the statistical data collected. The statistical analysis is based upon the probability of the success rate that is generated and calculated as the result of the research scenarios.

The scenario where the user had misplaced the device at home location and the iPhone was needed to be located. The conditions were that the iPhone was at home location but was misplaced and needed to be located. There are two conditions available for this scenario: the iPhone is in the online mode and the iPhone is in the offline mode. The iPhone in the offline mode did not seem to respond efficiently when the network was completely available. Out of ten test attempts, five test attempts were a failure. The preceding table explains the same. The iPhone is not efficiently responding when the mobile data connection is not stable in availability. The offline requests made were not successful in reaching the device.

Some tests failed by delay in time while some requests did not reach the iPhone at all.

The scenario where the user had lost the device (assumed) at some location, say Z, and the user needed to locate the iPhone. The condition was that the iPhone is misplaced at Z location. Now the user wants to locate the iPhone. The mode that is available to the iPhone in this scenario is online and offline. This scenario is without using the tracking functionality. A custom user message is displayed on the iPhone screen and the device is located on the web portal of iCloud. The iPhone in the offline mode did not seem to respond efficiently when the network was completely available. Out of ten test attempts, around seven test attempts were a failure. The preceding table explains the same. The iPhone was not able to respond efficiently when it was trying to enter a network. The network was a bit unstable and caused multiple issues. Some requests made by the user from the web portal did not reach the iPhone, while the others were delayed in reaching the iPhone.

The scenario where the user had lost the device (assumed) at some location, say X, and the user needed to locate the iPhone and also track it. The conditions were that the iPhone is at X location and is lost and the user needs the iPhone to be located and tracked. The mode that is available to the iPhone in this scenario is online and offline. This scenario is using the tracking functionality, unlike the previous scenario. A custom user message is displayed on the iPhone screen, which is similar to scenario two, and the device is located and tracked on the web portal of iCloud. The iPhone in the offline mode did not seem to respond efficiently when the network was completely available. Out of ten test attempts, around four test attempts were a failure. The preceding table explains the same. The iPhone was not able to respond efficiently when it was trying to enter a network. The network was a bit unstable and caused multiple issues. Some requests made by the user from the web portal did not reach the iPhone, while the others were delayed in reaching the iPhone. The tracking would stop in the midway even when the network was available and also that the iPhone was not able to receive the network properly.

Sometimes, the GPS service was not able to broadcast the location efficiently, thereby giving false and wrong information sometimes. The GPS service was efficient only when out in the open and not inside any building or structure.

V Conclusion

The application used for the research is completely dependent on the connectivity and availability of the internet connection either through the mobile data network, provided by the network or service provider, or the Wi-Fi connection. If any commands are issued by the user, those will be executed only when the device reconnects to the internet or comes online. The commands are queued in for execution at the server end, waiting for the device to reconnect. This is a limitation where in the data services are unavailable; the application cannot perform its task. Anyone can misuse this vulnerability of this iPhone and harm the data or forge the data and personal information available on the iPhone, thereby threatening the information security of the personal data available on the iPhone. Hence, it is required that some other mechanism or service should be introduced or constructed or developed using which this limitation can be overcome and the users of Apple's product will be able to get the maximum benefit of the iCloud services provided by Apple Inc.

The limitations of the application are the inability to access the internet at some intervals of time. Apple Inc can improve the reliability of the Find My iPhone application by sending an encrypted text messages (for example SMS) to the online services and receiving these messages from the iPhone to recognize the commands that are executed or that need to be executed.

The Find My iPhone application is nothing but a software program. A software program cannot be completely bug-free at any point of time. There are some loopholes in the software which can be seen and found out only when the user is trying for it multiple times. The major issue is caused by the mobile data network or the Wi-Fi network required for the internet connection. Despite the mobile network availability, the

iPhone fails to connect to the internet due to any circumstances such as bad weather, network failure, and so on. All the results are falling under the failure rate because of the internet network connectivity failure. If any commands are issued by the user, those will be executed when the device reconnects to the internet or comes online. The commands are queued in for execution at the server end, waiting for the device to reconnect. This is a limitation where in the data services are unavailable; the application cannot perform its task.

References

- 1) Apple. (2012). What is iCloud. Retrieved from <http://www.apple.com/icloud/what-is.html>
- 2) Baran, D. (2011, June 7). Apple iCloud. What it is & the benefits. Retrieved from <http://www.webguild.org/20110607/apple-icloud-what-is-it-what-are-the-benefits>
- 3) Smith, J. (2011, October 11). iOS 5: What is iCloud and what will it do for me? Retrieved from <http://www.gottabemobile.com/2011/10/11/ios-5-what-is-icloud-and-what-will-it-do-for-me/>
- 4) iCloud: iCloud security and privacy overview. (2013). Apple Inc. Retrieved from <http://support.apple.com/kb/HT4865>
- 5) Steve Jobs. (2013). The Biography Channel website. Retrieved 04:28, Mar 03, 2013, from <http://www.biography.com/people/steve-jobs-9354805>
- 6) iOS. Details of versions of iOS on iPhone and other iOS devices. Retrieved from <http://en.wikipedia.org/wiki?curid=2632126>
- 7) <https://support.apple.com/en-in/HT201365>
- 8) iCloud: What is iCloud? Retrieved from <https://support.apple.com/kb/PH2697>; https://support.apple.com/kb/PH2698?viewlocale=en_US; [https://discussions.apple.com/thread/6852417?start=0&start=0](https://discussions.apple.com/thread/6852417?start=0&start=0;); https://support.apple.com/kb/PH2698?viewlocale=en_US&locale=en_AU; <http://www.slideshare.net/munaani/icloud-computing-seminar>

- 9) iPhone: what is iPhone? Details of iPhone. Specifications of iPhone. Retrieved from <https://discussions.apple.com/thread/7018518?start=0&start=0;http://en.wikipedia.org/wiki?curid=2632126>
- 10)Find My iPhone: how to use Find My iPhone. Retrieved from <http://favfind.xyz/find-my-iphone-login/>; https://support.apple.com/kb/PH2701?viewlocale=en_US&locale=en_US;
<https://support.apple.com/kb/ph2701>
- 11)Activation Lock. Usage of activation lock. Retrieved from <http://apple.stackexchange.com/questions/127645/how-can-i-know-if-my-iphone-had-been-erased>;
<https://support.apple.com/en-us/HT201365>
- 12)Finding issues for the Find My iPhone application. Retrieved from <https://www.swisscom.ch/en/business/sme/help/loesung/aktivierungssperre-mein-iphone-suchen.html>;
<http://www.intego.com/mac-security-blog/how-to-enable-the-kill-switch-on-your-iphone-or-ipad/>; iCloud: iCloud security and privacy overview. (2013). Apple Inc. Retrieved from <http://support.apple.com/kb/HT4865>
- 13)<http://awhite16-icloud.blogspot.in/2012/11/research-paper-on-icloud-technology.html>
- 14)<http://trendblog.net/how-to-track-your-lost-iphone-or-ipad-without-tracking-app/>
- 15)<http://it103jacobshepherd.blogspot.com/>
- 16)<http://citeseerx.ist.psu.edu/showciting?cid=10209151>
- 17)<http://hercent.com/category/uncategorized/page/12273/>
- 18)http://www.researchgate.net/profile/Robin_Walia/publication/265583259_CLOUD_COMPUTING_THEIR_BENEFITS_TO_FUTURE_APPLICATIONS/links/551ff4b80cf2a2d9e141a735.pdf
- 19)<http://cirworld.org/journals/index.php/ijct/article/download/1156/pdf>
- 20)<http://en.wikipedia.org/wiki?curid=2632126>
- 21)<https://bay179.mail.live.com/?tid=cmEHjJZoIE5RGZGwAhWthTDg2&fid=flinbox>



Sanjay Agal was born in salumber village of udaipur city in 1984. He received his BE in Information Technology and MTech in Computer Science in 2008 and 2012 from Rajasthan University and Mewar University. From 2008 to 2012 he was

assistant professor at pacific college of engineering and from 2012 to till now he is working as associate professor and head of Department computer science. His research interest includes Java , GIs , Artificial Intelligence.



Sampreshita Maheshwari was born in Jalgaon Maharatra. she completed her early education in Mumbai and then she completed a Diploma in Technology with specialization in Information Technology from Pravin

Rohidas Patil Polytechnic in 2009. Then she received a Bachelor's degree in Engineering with specialization in Information Technology from Shivaji University in the year 2012. She completed her Master of Technology in 2015, with specialization in Computer Science. She is currently working in InteractCRM Pvt. Ltd., Mumbai, as a Software Engineer in the Implementation and Support Division of the Solution Delivery Group, since 10 months. she have a strong passion towards his research and her research area includes Information technology and software engineering, she is a keen student of soft computing. this paper is a introductory paper with idevice and apple technology analysis.

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGILIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Dr. Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Dr Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Dr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Dr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Dr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Dr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Dr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Dr. P. Vasant, University Technology Petronas, Malaysia
Dr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Dr. Praveen Ranjan Srivastava, BITS PILANI, India
Dr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Dr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Dr. Tirthankar Gayen, IIT Kharagpur, India
Dr. Huei-Ru Tseng, National Chiao Tung University, Taiwan

Prof. Ning Xu, Wuhan University of Technology, China
Dr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen
& Universiti Teknologi Malaysia, Malaysia.
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India
Dr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan
Prof. Syed S. Rizvi, University of Bridgeport, USA
Dr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India
Dr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal
Dr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P
Dr. Poonam Garg, Institute of Management Technology, India
Dr. S. Mehta, Inha University, Korea
Dr. Dilip Kumar S.M, Bangalore University, Bangalore
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia
Dr. Saqib Saeed, University of Siegen, Germany
Dr. Pavan Kumar Gorakavi, IPMA-USA [YC]
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India
Dr. J. Komala Lakshmi, SNR Sons College, Computer Science, India
Dr. Muhammad Sohail, KUST, Pakistan
Dr. Manjaiah D.H, Mangalore University, India
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada
Dr. Deepak Laxmi Narasimha, University of Malaya, Malaysia
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India
Dr. M. Azath, Anna University, India
Dr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh
Dr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia
Dr Suresh Jain, Devi Ahilya University, Indore (MP) India,
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia
Dr. Hanumanthappa. J. University of Mysore, India
Dr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)
Dr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria
Dr. Santosh K. Pandey, The Institute of Chartered Accountants of India
Dr. P. Vasant, Power Control Optimization, Malaysia
Dr. Petr Ivankov, Automatika - S, Russian Federation
Dr. Utkarsh Seetha, Data Infosys Limited, India
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore
Assist. Prof. A. Neela madheswari, Anna university, India

Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh
Dr. Atul Gonsai, Saurashtra University, Gujarat, India
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand
Mrs. G. Nalini Priya, Anna University, Chennai
Dr. P. Subashini, Avinashilingam University for Women, India
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat
Mr Jitendra Agrawal, : Rajiv Gandhi Proudhyogiki Vishwavidyalaya, Bhopal
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai
Assist. Prof, Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah
Mr. Nitin Bhatia, DAV College, India
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia
Assist. Prof. Sonal Chawla, Panjab University, India
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology, Durban,South Africa
Prof. Mydhili K Nair, Visweswaraiiah Technological University, Bangalore, India
M. Prabu, Adhiyamaan College of Engineering/Anna University, India
Mr. Swakkhar Shatabda, United International University, Bangladesh
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan
Mr. H. Abdul Shabeer, I-Nautix Technologies,Chennai, India
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran
Mr. Zeashan Hameed Khan, Université de Grenoble, France
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India
Dr. Maslin Masrom, University Technology Malaysia, Malaysia
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City
Dr. Mary Lourde R., BITS-PILANI Dubai , UAE
Dr. Abdul Aziz, University of Central Punjab, Pakistan

Mr. Karan Singh, Gautam Budtha University, India
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia
Assistant Prof. Yasser M. Alginahi, Taibah University, Madinah Munawwarah, KSA
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India
Dr. Mana Mohammed, University of Tlemcen, Algeria
Prof. Jatinder Singh, Universal Institutiion of Engg. & Tech. CHD, India
Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim
Dr. Bin Guo, Institute Telecom SudParis, France
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India
Dr. C. Arun, Anna University, India
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology
Subhabrata Barman, Haldia Institute of Technology, West Bengal
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand
Dr. P. Chakrabarti, Sir Padampat Singhanian University, Udaipur, India
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India

Mr. Serguei A. Mokhov, Concordia University, Canada
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA
Dr. S. Karthik, SNS College of Technology, India
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain
Mr. A.D.Potgantwar, Pune University, India
Dr. Himanshu Aggarwal, Punjabi University, India
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai
Dr. Prasant Kumar Pattnaik, KIST, India.
Dr. Ch. Aswani Kumar, VIT University, India
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA
Mr. Arun Kumar, Sir Padam Pat Singhania University, Udaipur, Rajasthan
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan
Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA
Mr. R. Jagadeesh Kannan, RMK Engineering College, India
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India
Dr. F.Sagayaraj Francis, Pondicherry Engineering College, India
Dr. Ajay Goel, HIET , Kaithal, India
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India
Mr. Suhas J Manangi, Microsoft India
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded , India
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India
Dr. Amjad Rehman, University Technology Malaysia, Malaysia
Mr. Rachit Garg, L K College, Jalandhar, Punjab
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan
Dr. Thorat S.B., Institute of Technology and Management, India
Mr. Ajay Prasad, Sir Padampat Singhania University, Udaipur, India
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh

Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA
Mr. Anand Kumar, AMC Engineering College, Bangalore
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India
Dr. V V S S S Balaram, Sreenidhi Institute of Science and Technology, India
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India
Prof. Niranjana Reddy, P, KITS, Warangal, India
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India
Dr. A.Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India
Dr. Lena Khaled, Zarqa Private University, Aman, Jordan
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India
Dr. Tossapon Boongoen, Aberystwyth University, UK
Dr. Bilal Alatas, Firat University, Turkey
Assist. Prof. Jyoti Praaksh Singh, Academy of Technology, India
Dr. Ritu Soni, GNG College, India
Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.
Dr. Binod Kumar, Lakshmi Narayan College of Tech.(LNCT) Bhopal India
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan
Dr. T.C. Manjunath, ATRIA Institute of Tech, India
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan
Assist. Prof. Harmunish Taneja, M. M. University, India
Dr. Chitra Dhawale, SICSR, Model Colony, Pune, India
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India
Mr. G. Appasami, Dr. Pauls Engineering College, India
Mr. M Yasin, National University of Science and Tech, Karachi (NUST), Pakistan
Mr. Yaser Miaji, University Utara Malaysia, Malaysia
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh
Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India
Dr. S. Sasikumar, Roever Engineering College
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India
Mr. Nwaocha Vivian O, National Open University of Nigeria
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India
Mr. Kunal Chadha, R&D Software Engineer, Gemalto, Singapore

Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia
Dr. Dhuha Basheer abdullah, Mosul university, Iraq
Mr. S. Audithan, Annamalai University, India
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam
Assist. Prof. Anand Sharma, MITS, Lakshmangarh, Sikar, Rajasthan, India
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad
Mr. Deepak Gour, Sir Padampat Singhania University, India
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India
Mr. Ali Balador, Islamic Azad University, Iran
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India
Dr. Debojyoti Mitra, Sir padampat Singhania University, India
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia
Mr. Zhao Zhang, City University of Hong Kong, China
Prof. S.P. Setty, A.U. College of Engineering, India
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India
Dr. Hanan Elazhary, Electronics Research Institute, Egypt
Dr. Hosam I. Faiq, USM, Malaysia
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India
Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya
Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.
Dr. Kasarapu Ramani, JNT University, Anantapur, India
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India
Dr. C G Ravichandran, R V S College of Engineering and Technology, India
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India

Dr. Nikolai Stoianov, Defense Institute, Bulgaria
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia
Dr. Nighat Mir, Effat University, Saudi Arabia
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India
Mr. P. Sivakumar, Anna university, Chennai, India
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia
Mr. Nikhil Patrick Lobo, CADES, India
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India
Assist. Prof. Vishal Bharti, DCE, Gurgaon
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India
Mr. Hamed Taherdoost, Tehran, Iran
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran
Mr. Shantanu Pal, University of Calcutta, India
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria
Mr. P. Mahalingam, Caledonian College of Engineering, Oman
Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt
Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India
Mr. Muhammad Asad, Technical University of Munich, Germany
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran
Prof. S. V. Nagaraj, RMK Engineering College, India
Mr. Ashikali M Hasan, Senior Researcher, CeINet security, India

Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India
Dr. Jagdish B. Helonde, Nagpur University/ITM college of engg, Nagpur, India
Professor, Doctor BOUHORMA Mohammed, University Abdelmalek Essaadi, Morocco
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India
Mr. Sunil Taneja, Kurukshetra University, India
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia
Dr. Yaduvir Singh, Thapar University, India
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran
Assoc. Prof. Dharendra Mishra, SVKM's NMIMS University, India
Prof. Shapoor Zarei, UAE Inventors Association, UAE
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India
Prof. Anant J Umbarkar, Walchand College of Engg., India
Assist. Prof. B. Bharathi, Sathyabama University, India
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore
Prof. Walid Moudani, Lebanese University, Lebanon
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India
Associate Prof. Dr. Manuj Darbari, BBD University, India
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India
Dr. Abhay Bansal, Amity School of Engineering & Technology, India
Ms. Sumita Mishra, Amity School of Engineering and Technology, India
Professor S. Viswanadha Raju, JNT University Hyderabad, India
Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia
Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India

Mr. Shervan Fekri Ershad, Shiraz International University, Iran
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India
Ms. Sarla More, UIT, RGTU, Bhopal, India
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India
Dr. M. N. Giri Prasad, JNTUCE, Pulivendula, A.P., India
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India
Assist. Prof. Navnish Goel, S. D. College Of Enginnering & Technology, India
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan
Mr. Mohammad Asadul Hoque, University of Alabama, USA
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina
Dr S. Rajalakshmi, Botho College, South Africa
Dr. Mohamed Sarrab, De Montfort University, UK
Mr. Basappa B. Kodada, Canara Engineering College, India
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India
Dr . G. Singaravel, K.S.R. College of Engineering, India
Dr B. G. Geetha, K.S.R. College of Engineering, India
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India
Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India
Assist. Prof. Maram Balajee, GMRIT, India

Assist. Prof. Monika Bhatnagar, TIT, India
Prof. Gaurang Panchal, Charotar University of Science & Technology, India
Prof. Anand K. Tripathi, Computer Society of India
Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India
Assist. Prof. Supriya Raheja, ITM University, India
Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.
Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India
Prof. Mohan H.S, SJB Institute Of Technology, India
Mr. Hossein Malekinezhad, Islamic Azad University, Iran
Mr. Zatin Gupta, Universti Malaysia, Malaysia
Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India
Assist. Prof. Ajal A. J., METS School Of Engineering, India
Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria
Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India
Md. Nazrul Islam, University of Western Ontario, Canada
Tushar Kanti, L.N.C.T, Bhopal, India
Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India
Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh
Dr. Kashif Nisar, University Utara Malaysia, Malaysia
Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA
Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan
Assist. Prof. Apoorvi Sood, I.T.M. University, India
Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia
Mr. Swapnil Sonar, Truba Institute College of Engineering & Technology, Indore, India
Ms. Yogita Gigras, I.T.M. University, India
Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College
Assist. Prof. K. Deepika Rani, HITAM, Hyderabad
Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India
Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad
Prof. Dr.S.Saravanan, Muthayammal Engineering College, India
Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran
Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India
Assist. Prof. P.Oliver Jayaprakash, Anna University, Chennai
Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India
Dr. Asoke Nath, St. Xavier's College, India
Mr. Masoud Rafighi, Islamic Azad University, Iran
Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India
Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India
Mr. Sandeep Maan, Government Post Graduate College, India
Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India
Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India
Mr. R. Balu, Bharathiar University, Coimbatore, India

Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India
Prof. P. Senthilkumar, Vivekanandha Institute of Engineering and Technology for Woman, India
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran
Mr. Laxmi chand, SCTL, Noida, India
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad
Prof. Mahesh Panchal, KITRC, Gujarat
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode
Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhania University, India
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technology, India
Mr. Srikantha Kumar Mohapatra, NMIET, Orissa, India
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India
Mr. G. Premsankar, Ericsson, India
Assist. Prof. T. Hemalatha, VELS University, India
Prof. Tejaswini Apte, University of Pune, India
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India
Mr. Vorugunti Chandra Sekhar, DA-IICT, India
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia
Dr. Aderemi A. Atayero, Covenant University, Nigeria
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India
Mr. Hassen Mohammed Abdulllah Alsafi, International Islamic University Malaysia (IIUM) Malaysia
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan
Mr. R. Balu, Bharathiar University, Coimbatore, India
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India
Prof. K. Saravanan, Anna university Coimbatore, India
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN
Assoc. Prof. S. Asif Hussain, AITS, India

Assist. Prof. C. Venkatesh, AITS, India
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan
Dr. B. Justus Rabi, Institute of Science & Technology, India
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India
Mr. Alejandro Mosquera, University of Alicante, Spain
Assist. Prof. Arjun Singh, Sir Padampat Singhanian University (SPSU), Udaipur, India
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India
Mr. Hassen Mohammed Abdullah Alsafi, International Islamic University Malaysia (IIUM)
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu
Dr. K. Reji Kumar, N S S College, Pandalam, India
Assoc. Prof. K. Seshadri Sastry, EIILM University, India
Mr. Kai Pan, UNC Charlotte, USA
Mr. Ruikar Sachin, SGGSIET, India
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt
Assist. Prof. Amanpreet Kaur, ITM University, India
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia
Dr. Abhay Bansal, Amity University, India
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA
Assist. Prof. Nidhi Arora, M.C.A. Institute, India
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India
Dr. S. Sankara Gomathi, Panimalar Engineering college, India
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India
Dr. Lamri LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India
Mr. Ram Kumar Singh, S.V Subharti University, India

Assistant Prof. Sunish Kumar O S, Amaljiyothi College of Engineering, India
Dr Sanjay Bhargava, Banasthali University, India
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India
Mr. Roohollah Etemadi, Islamic Azad University, Iran
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria
Mr. Sumit Goyal, National Dairy Research Institute, India
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur
Dr. S.K. Mahendran, Anna University, Chennai, India
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab
Dr. Ashu Gupta, Apeejay Institute of Management, India
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus
Mr. Maram Balajee, GMR Institute of Technology, India
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria
Mr. Jasvir Singh, University College Of Engg., India
Mr. Vivek Tiwari, MANIT, Bhopal, India
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India
Mr. Somdip Dey, St. Xavier's College, Kolkata, India
Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh
Mr. Sathyapraksh P., S.K.P Engineering College, India
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India
Mr. Md. Abdul Ahad, K L University, India
Mr. Vikas Bajpai, The LNM IIT, India
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai
Mr. A. Siles Balasingh, St. Joseph University in Tanzania, Tanzania
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India
Mr. Kumar Dayanand, Cambridge Institute of Technology, India
Dr. Syed Asif Ali, SMI University Karachi, Pakistan
Prof. Pallvi Pandit, Himachal Pradesh University, India
Mr. Ricardo Verschueren, University of Gloucestershire, UK
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India
Dr. S. Sumathi, Anna University, India

Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India
Assist. Prof M. Anand Kumar, Karpagam University, Coimbatore, India
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat
Mr. Sivakumar, Codework solutions, India
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA
Mr. Varadala Sridhar, Varadhaman College Engineering College, Affiliated To JNTU, Hyderabad
Assist. Prof. Manoj Dhawan, SVITS, Indore
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India
Dr. S. Santhi, SCSVMV University, India
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh
Mr. Sandeep Reddivari, Mississippi State University, USA
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal
Dr. Hazra Imran, Athabasca University, Canada
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India
Ms. Jaspreet Kaur, Distance Education LPU, India
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India
Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India
Mr. Khaldi Amine, Badji Mokhtar University, Algeria
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany
Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India
Dr. Nadir Bouchama, CERIST Research Center, Algeria
Dr. R. Sathishkumar, Sri Venkateswara College of Engineering, India
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco
Dr. S. Malathi, Panimalar Engineering College, Chennai, India
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India

Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India
Dr. Hamza Aldabbas, Al-Balqa'a Applied University, Jordan
Dr. G. Rasitha Banu, Vel's University, Chennai
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India
Ms. U. Sinthuja, PSG college of arts & science, India
Dr. Ehsan Saradar Torshizi, Urmia University, Iran
Dr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim
Dr. Khaled Eskaf, Arab Academy for Science ,Technology & Maritime Transportation, Egypt
Dr. Nishant Gupta, University of Jammu, India
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India
Assistant Prof. Tribikram Pradhan, Manipal Institute of Technology, India
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India
Dr. Rahul Malik, Cisco Systems, USA
Dr. S. C. Lingareddy, ALPHA College of Engineering, India
Assistant Prof. Mohammed Shuaib, Interl University, Lucknow, India
Dr. Sachin Yele, Sanghvi Institute of Management & Science, India
Dr. T. Thambidurai, Sun Univercell, Singapore
Prof. Anandkumar Telang, BKIT, India
Assistant Prof. R. Poorvadevi, SCSVMV University, India
Dr Uttam Mande, Gitam University, India
Dr. Poornima Girish Naik, Shahu Institute of Business Education and Research (SIBER), India
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India
Dr. Mohammed Zuber, AISECT University, India
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia
Dr. K. R. Ananth, Velalar College of Engineering and Technology, India
Assistant Prof. Sanjay Sharma, Roorkee Engineering & Management Institute Shamli (U.P), India
Assistant Prof. Panem Charan Arur, Priyadarshini Institute of Technology, India
Dr. Ashwak Mahmood muhsen alabaichi, Karbala University / College of Science, Iraq
Dr. Urmila Shrawankar, G H Raison College of Engineering, Nagpur (MS), India
Dr. Krishan Kumar Paliwal, Panipat Institute of Engineering & Technology, India
Dr. Mukesh Negi, Tech Mahindra, India
Dr. Anuj Kumar Singh, Amity University Gurgaon, India
Dr. Babar Shah, Gyeongsang National University, South Korea
Assistant Prof. Jayprakash Upadhyay, SRI-TECH Jabalpur, India
Assistant Prof. Varadala Sridhar, Vidya Jyothi Institute of Technology, India
Assistant Prof. Parameshachari B D, KSIT, Bangalore, India
Assistant Prof. Ankit Garg, Amity University, Haryana, India

Assistant Prof. Rajashe Karappa, SDMCET, Karnataka, India
Assistant Prof. Varun Jasuja, GNIT, India
Assistant Prof. Sonal Honale, Abha Gaikwad Patil College of Engineering Nagpur, India
Dr. Pooja Choudhary, CT Group of Institutions, NIT Jalandhar, India
Dr. Faouzi Hidoussi, UHL Batna, Algeria
Dr. Naseer Ali Husieen, Wasit University, Iraq
Assistant Prof. Vinod Kumar Shukla, Amity University, Dubai
Dr. Ahmed Farouk Metwaly, K L University
Mr. Mohammed Noaman Murad, Cihan University, Iraq
Dr. Suxing Liu, Arkansas State University, USA
Dr. M. Gomathi, Velalar College of Engineering and Technology, India
Assistant Prof. Sumardiono, College PGRI Blitar, Indonesia
Dr. Latika Kharb, Jagan Institute of Management Studies (JIMS), Delhi, India
Associate Prof. S. Raja, Pauls College of Engineering and Technology, Tamilnadu, India
Assistant Prof. Seyed Reza Pakize, Shahid Sani High School, Iran
Dr. Thiyaagu Nagaraj, University-INOUE, India
Assistant Prof. Noreen Sarai, Harare Institute of Technology, Zimbabwe
Assistant Prof. Gajanand Sharma, Suresh Gyan Vihar University Jaipur, Rajasthan, India
Assistant Prof. Mapari Vikas Prakash, Siddhant COE, Sudumbare, Pune, India
Dr. Devesh Katiyar, Shri Ramswaroop Memorial University, India
Dr. Shenshen Liang, University of California, Santa Cruz, US
Assistant Prof. Mohammad Abu Omar, Limkokwing University of Creative Technology- Malaysia
Mr. Snehasis Banerjee, Tata Consultancy Services, India
Assistant Prof. Kibona Lusekelo, Ruaha Catholic University (RUCU), Tanzania
Assistant Prof. Adib Kabir Chowdhury, University College Technology Sarawak, Malaysia
Dr. Ying Yang, Computer Science Department, Yale University, USA
Dr. Vinay Shukla, Institute Of Technology & Management, India
Dr. Liviu Octavian Maftciu-Scai, West University of Timisoara, Romania
Assistant Prof. Rana Khudhair Abbas Ahmed, Al-Rafidain University College, Iraq
Assistant Prof. Nitin A. Naik, S.R.T.M. University, India
Dr. Timothy Powers, University of Hertfordshire, UK
Dr. S. Prasath, Bharathiar University, Erode, India
Dr. Ritu Shrivastava, SIRTH Bhopal, India
Prof. Rohit Shrivastava, Mittal Institute of Technology, Bhopal, India
Dr. Gianina Mihai, Dunarea de Jos" University of Galati, Romania
Assistant Prof. Ms. T. Kalai Selvi, Erode Sengunthar Engineering College, India
Assistant Prof. Ms. C. Kavitha, Erode Sengunthar Engineering College, India
Assistant Prof. K. Sinivasamoorthi, Erode Sengunthar Engineering College, India
Assistant Prof. Mallikarjun C Sarsamba Bheemna Khandre Institute Technology, Bhalki, India
Assistant Prof. Vishwanath Chikaraddi, Veermata Jijabai technological Institute (Central Technological Institute), India
Assistant Prof. Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, India

Assistant Prof. Mohammed Noaman Murad, Cihan University, Iraq
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Dr. Parul Verma, Amity University, India
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco
Assistant Prof. Madhavi Dhingra, Amity University, Madhya Pradesh, India
Assistant Prof.. G. Selvavinayagam, SNS College of Technology, Coimbatore, India
Assistant Prof. Madhavi Dhingra, Amity University, MP, India
Professor Kartheesan Log, Anna University, Chennai
Professor Vasudeva Acharya, Shri Madhwa vadiraja Institute of Technology, India
Dr. Asif Iqbal Hajamydeen, Management & Science University, Malaysia
Assistant Prof., Mahendra Singh Meena, Amity University Haryana
Assistant Professor Manjeet Kaur, Amity University Haryana
Dr. Mohamed Abd El-Basset Matwalli, Zagazig University, Egypt
Dr. Ramani Kannan, Universiti Teknologi PETRONAS, Malaysia
Assistant Prof. S. Jagadeesan Subramaniam, Anna University, India
Assistant Prof. Dharmendra Choudhary, Tripura University, India
Assistant Prof. Deepika Vodnala, SR Engineering College, India
Dr. Kai Cong, Intel Corporation & Computer Science Department, Portland State University, USA
Dr. Kailas R Patil, Vishwakarma Institute of Information Technology (VIIT), India
Dr. Omar A. Alzubi, Faculty of IT / Al-Balqa Applied University, Jordan
Assistant Prof. Kareemullah Shaik, Nimra Institute of Science and Technology, India
Assistant Prof. Chirag Modi, NIT Goa
Dr. R. Ramkumar, Nandha Arts And Science College, India
Dr. Priyadharshini Vydhialingam, Harathiar University, India
Dr. P. S. Jagadeesh Kumar, DBIT, Bangalore, Karnataka
Dr. Vikas Thada, AMITY University, Pachgaon
Dr. T. A. Ashok Kumar, Institute of Management, Christ University, Bangalore
Dr. Shaheera Rashwan, Informatics Research Institute
Dr. S. Preetha Gunasekar, Bharathiyar University, India
Asst Professor Sameer Dev Sharma, Uttaranchal University, Dehradun
Dr. Zhihan Lv, Chinese Academy of Science, China
Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, Amritsar
Dr. Umar Ruhi, University of Ottawa, Canada
Dr. Jasmin Cosic, University of Bihac, Bosnia and Herzegovina
Dr. Homam Reda El-Taj, University of Tabuk, Kingdom of Saudi Arabia
Dr. Mostafa Ghobaei Arani, Islamic Azad University, Iran
Dr. Ayyasamy Ayyanar, Annamalai University, India
Dr. Selvakumar Manickam, Universiti Sains Malaysia, Malaysia
Dr. Murali Krishna Namana, GITAM University, India
Dr. Smriti Agrawal, Chaitanya Bharathi Institute of Technology, Hyderabad, India
Professor Vimalathithan Rathinasabapathy, Karpagam College Of Engineering, India
Dr. Sushil Chandra Dimri, Graphic Era University, India

Dr. Dinh-Sinh Mai, Le Quy Don Technical University, Vietnam
Dr. S. Rama Sree, Aditya Engg. College, India
Dr. Ehab T. Alnfrawy, Sadat Academy, Egypt
Dr. Patrick D. Cerna, Haramaya University, Ethiopia
Dr. Vishal Jain, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), India
Associate Prof. Dr. Jiliang Zhang, North Eastern University, China
Dr. Sharefa Murad, Middle East University, Jordan
Dr. Ajeet Singh Poonia, Govt. College of Engineering & technology, Rajasthan, India
Dr. Vahid Esmaeelzadeh, University of Science and Technology, Iran
Dr. Jacek M. Czerniak, Casimir the Great University in Bydgoszcz, Institute of Technology, Poland
Associate Prof. Anisur Rehman Nasir, Jamia Millia Islamia University
Assistant Prof. Imran Ahmad, COMSATS Institute of Information Technology, Pakistan
Professor Ghulam Qasim, Preston University, Islamabad, Pakistan
Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women
Dr. Wencan Luo, University of Pittsburgh, US
Dr. Musa PEKER, Faculty of Technology, Mugla Sitki Kocman University, Turkey
Dr. Gunasekaran Shanmugam, Anna University, India
Dr. Binh P. Nguyen, National University of Singapore, Singapore
Dr. Rajkumar Jain, Indian Institute of Technology Indore, India
Dr. Imtiaz Ali Halepoto, QUEST Nawabshah, Pakistan
Dr. Shaligram Prajapat, Devi Ahilya University Indore India
Dr. Sunita Singhal, Birla Institute of Technology and Science, Pilani, India
Dr. Ijaz Ali Shoukat, King Saud University, Saudi Arabia

CALL FOR PAPERS

International Journal of Computer Science and Information Security

IJCSIS 2016
ISSN: 1947-5500

<http://sites.google.com/site/ijcsis/>

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity

Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc.), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on

its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embedded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at <http://sites.google.com/site/ijcsis/authors-notes> .



© IJCSIS PUBLICATION 2016

ISSN 1947 5500

<http://sites.google.com/site/ijcsis/>